CONSILIUL

DIRECȚI



codificare decodificare

13 VOLUME

CONSILIUL SECURITĂŢII STATULUI
DIRECŢIA PERSONAL ŞI ÎNVĂŢĂMÎNT

Pentru uz intern

CODIFICARE, DECODIFICARE

Seria 1020

1970

Traducere de lt. IOAN ROTAR
Coperta executată de FLORIN DUDESCU

DIN PARTEA REDACȚIEI

Lucrarea „Codificare, decodificare" are menirea de a prezenta cititorilor unele aspecte din evoluția, de-a lungul veacurilor, a unei științe cu tente de mister, ce a fascinat și a atras imaginația celor mai diverse minți, născute în civilizațiile care au stăruit pe meridianele globului.

Apărută pe malurile Nilului, criptologia avea să răspundă nevoii de a apăra și de a afla secrete ce constituiau interese vitale ale unor țări, popoare, grupări sociale, politice, religioase etc. Astfel, încă de la început, s-au conturat cele două componente de bază ale noii științe și anume: criptografia și criptanaliza. Scopul criptografiei este ca, prin transformarea deliberată a scrisului, să se ascundă înțelesul unor mesaje față de cei ce nu trebuie să-l cunoască, iar criptanaliza urmărește să descopere această transformare. Rezultă, deci, interdependența dintre aceste două ramuri ale criptologiei, fiind foarte ușor de înțeles că orice schimbare, în sens progresiv, în una dintre ele atrage după sine schimbări evolutive și în cealaltă. O astfel de axiomă este ilustrată de istoria criptologiei, căci, de la elementele primare, cuprinse în culturile antice, pînă la mașinile electronice din zilele noastre, a fost parcurs un drum în general ascendent, presărat, însă, cu multe suișuri și coborîșuri abrupte.

În această lucrare sînt prezentate numai momentele de ascensiune ale criptologiei. S-a procedat în acest mod, pe de o parte, pentru a prezenta sistematic și logic dezvoltarea, de-a

lungul timpului, a celor două ramuri ale criptologiei, iar pe de altă parte, pentru a ajuta la o mai bună înțelegere a sistemelor, procedeelor și metodelor de criptare și decriptare moderne, respectîndu-se principiul didactic, conform căruia, în însușirea unor cunoștințe, trebuie să se pornească de la simplu pentru a se ajunge la complex.

Scopul lucrării este, deci, să-l înarmeze pe cititor cu o serie de cunoștințe din domeniul cifrurilor, codurilor și al altor procedee folosite în scrierile ascunse.

Ea are menirea să stimuleze interesul față de acest domeniu de activitate și să atragă atenția asupra pericolului ce rezidă în tratarea cu superficialitate a măsurilor de apărare a secretelor de partid, de stat și militare, indicînd armele care stau la dispoziția oricui este interesat să apere sau să intre în posesia acestor secrete.

Din lucrare emană, de asemenea, caracterul evolutiv al criptologiei, fapt care îndeamnă pe fiecare să încerce să-și aducă contribuția activă la dezvoltarea acestei științe, atît prin elaborarea unor noi sisteme de criptare, cît și prin găsirea unor metode ingenioase de soluționare a criptogramelor și scrierilor ascunse, folosite în mod curent în activitatea subversivă.

NAȘTEREA CRIPTOLOGIEI

PRIMII 3 000 DE ANI

Cu aproape 4 000 de ani în urmă, într-un oraș numit Menet Khufu, de pe malul Nilului, un scrib, desenînd hieroglife, povestea viața stăpînului său și — făcînd acest lucru — scria primele rînduri din istoria criptologiei.

Nu era vorba de un sistem de scriere secretă de tipul celui cunoscut de lumea modernă, ci de folosirea unor hieroglife mai deosebite pentru a proslăvi faptele stăpînului. De asemenea, intenția lui nu era să facă textul de neînțeles, ci să-i acorde grandoare, demnitate și autoritate. Deci, nu se poate spune că acest text constituia o scriere secretă, dar el încorpora unul din elementele esențiale ale criptografiei: transformarea deliberată a scrisului.

Cu timpul, textele de acest gen s-au înmulțit, transformările s-au complicat și n-a trecut mult pînă cînd a apărut și cel de-al doilea element esențial al criptologiei: secretul.

Transformarea scrierii și secretul au dus la criptografie, deși la început aceasta se asemăna mai mult cu un joc prin care se urmărea să se întîrzie înțelegerea textului, iar criptanaliza nu era altceva decît rezolvarea unui rebus.

Așa a apărut criptologia, care, timp de 3 000 de ani, s-a dezvoltat, mai mult independent, în diferite părți ale lumii și multe realizări din acest domeniu au dispărut o dată cu apusul

lungul timpului, a celor două ramuri ale criptologiei, iar pe de altă parte, pentru a ajuta la o mai bună înţelegere a sistemelor, procedeelor şi metodelor de criptare şi decriptare moderne, respectîndu-se principiul didactic, conform căruia, în însuşirea unor cunoştinţe, trebuie să se pornească de la simplu pentru a se ajunge la complex.

Scopul lucrării este, deci, să-l înarmeze pe cititor cu o serie de cunoştinţe din domeniul cifrurilor, codurilor şi al altor procedee folosite în scrierile ascunse.

Ea are menirea să stimuleze interesul faţă de acest domeniu de activitate şi să atragă atenţia asupra pericolului ce rezidă în tratarea cu superficialitate a măsurilor de apărare a secretelor de partid, de stat şi militare, indicînd armele care stau la dispoziţia oricui este interesat să apere sau să intre în posesia acestor secrete.

Din lucrare emană, de asemenea, caracterul evolutiv al criptologiei, fapt care îndeamnă pe fiecare să încerce să-şi aducă contribuţia activă la dezvoltarea acestei ştiinţe, atît prin elaborarea unor noi sisteme de criptare, cît şi prin găsirea unor metode ingenioase de soluţionare a criptogramelor şi scrierilor ascunse, folosite în mod curent în activitatea subversivă.

NAŞTEREA CRIPTOLOGIEI

PRIMII 3 000 DE ANI

Cu aproape 4 000 de ani în urmă, într-un oraş numit Menet Khufu, de pe malul Nilului, un scrib, desenînd hieroglife, povestea viaţa stăpînului său şi — făcînd acest lucru — scria primele rînduri din istoria criptologiei.

Nu era vorba de un sistem de scriere secretă de tipul celui cunoscut de lumea modernă, ci de folosirea unor hieroglife mai deosebite pentru a proslăvi faptele stăpînului. De asemenea, intenţia lui nu era să facă textul de neînţeles, ci să-i acorde grandoare, demnitate şi autoritate. Deci, nu se poate spune că acest text constituia o scriere secretă, dar el încorpora unul din elementele esenţiale ale criptografiei: transformarea deliberată a scrisului.

Cu timpul, textele de acest gen s-au înmulţit, transformările s-au complicat şi n-a trecut mult pînă cînd a apărut şi cel de-al doilea element esenţial al criptologiei: secretul.

Transformarea scrierii şi secretul au dus la criptografie, deşi la început aceasta se asemăna mai mult cu un joc prin care se urmărea să se întîrzie înţelegerea textului, iar criptanaliza nu era altceva decît rezolvarea unui rebus.

Aşa a apărut criptologia, care, timp de 3 000 de ani, s-a dezvoltat, mai mult independent, în diferite părţi ale lumii şi multe realizări din acest domeniu au dispărut o dată cu apusul

unor civilizații. În alte părți, criptologia a supraviețuit, a intrat în cultura poporului respectiv și a continuat să progreseze. Dar progresul a fost anevoios și în salturi. Mai mult s-a pierdut decît s-a reținut. Abia în perioada Renașterii europene a început să se înalțe monumentul criptografic.

China, țara cu o cultură antică destul de dezvoltată, nu a acordat prea mare atenție criptografiei. Diplomații și autoritățile militare chineze se foloseau de curieri care memorau mesajele ce le aveau de transmis, iar pentru mesajele scrise foloseau mătase și hîrtie foarte subțire, care erau făcute cocoloș și învelite cu ceară. Curierul ascundea cocoloșul de ceară (de multe ori în rectum) sau îl înghițea, ducîndu-l astfel la destinatar.

Criptografia implica de cele mai multe ori folosirea unor coduri simple. De exemplu, dacă în numele unei persoane era inclusă ideograma „crizantemă", acesteia i se spunea codificat „floarea galbenă".

Pentru scopuri militare, în secolul al XI-lea, într-o compilație denumită „Problemele esențiale ale scrierilor clasicilor militari" se recomanda un cod, în accepțiunea modernă a cuvîntului. Astfel, pentru o listă de 40 de noțiuni în text clar: cereri de săgeți și arcuri, raportarea despre obținerea unei victorii etc. se foloseau primele 40 de ideograme ale unui poem. În cazul în care un comandant avea nevoie de săgeți, scria ideograma din poem corespunzătoare acestei noțiuni într-un anumit loc dintr-un mesaj obișnuit, îl sigila și-l trimitea celor în drept să-l primească. Răspunsul era dat sub aceeași formă. Dacă se întîmpla să cadă în mîna inamicului, mesajul respectiv nu putea fi descifrat decît dacă i se cunoștea codul. Cu toate acestea, în ciuda înaltei sale civilizații, China n-a strălucit prin realizări în domeniul criptologiei. Explicația constă și în aceea că scrierea chinezească, deși foarte veche, era foarte grea și cei care știau să o citească erau foarte puțini.

În India, de asemenea, se cunoșteau și, se pare, se practicau mai multe forme de comunicări secrete. Kautilya, presupusul autor al lucrării Artha-sastra, descriind serviciul de informații al Indiei, recomanda ofițerilor de spionaj să folosească scrierea secretă cînd dădeau misiuni agenților și spionilor. Pe de altă parte, recomanda ambasadorilor să folosească criptanaliza pentru a obține informații „decriptînd desenele și scrierile secrete".

Deși nu dă nici o metodă prin care puteau fi decriptate desenele și scrierile ascunse, faptul că vorbește despre soluțiile posibile ale acestora înseamnă că criptanaliza atinsese un stadiu destul de avansat. Oricum, este prima referire din istorie la criptanaliză folosită în scopuri politice.

Dar poate cea mai interesantă lucrare pentru criptologie este Kama-sutra, un manual de erotică, în care scrierea secretă este trecută ca una din cele 64 de arte pe care trebuie să le cunoască și să le practice femeile.

Se descriu două feluri de scriere secretă și anume: unul numit „Kautilyam", în care substituția literelor este bazată pe relații fonetice (vocalele devin consoane și invers), iar celălalt tip de scriere secretă constă din substituirea reciprocă doar a unui număr de litere-sunete, restul rămînînd neschimbate. De exemplu:

a k c t n m r e y
k a ț p n n ș s s
a este *k*, iar *k* este *a* etc.

În afară de aceste tipuri de criptografie, India antică folosea limba aluzivă, o formă de cod, precum și comunicarea cu ajutorul degetelor de la mînă, în care falangele substituiau consoanele, iar încheieturile vocalele.

A patra mare civilizație a antichității, cea din Mesopotamia, a atins, în criptografie, un nivel surprinzător pentru acele vremuri. Cea mai veche codificare este cuprinsă într-o tabletă de 7,5 x 5 cm și datează din anul 1 500 î.e.n.

Tableta conține cea mai veche formulă de fabricare a smalțului pentru vasele de lut. Scribul a folosit cuneiformele care aveau mai multe valori silabice, în sensul cel mai rar întîlnit. De asemenea, scribul a trunchiat sunetele, renunțînd la consoa-

nele finale ale unor semne silabice și a scris același cuvînt cu cuneiforme diferite în cadrul unui singur text.

Spre sfîrșitul civilizației mesopotamice, scribii au început să semneze înlocuind cuneiformele-silabe ale propriilor nume cu cifre. Cu timpul, diferite cuneiforme-silabe, cele foarte des uzitate, au început să fie substituite cu cifre chiar și în interiorul cuvintelor și asta nu pentru a ascunde înțelesul celor scrise, ci pentru a epata și a atrage atenția. Aceste tablete au fost foarte ușor descifrate de către asiriologi. Asiriologul englez Erle Leichty a descifrat mai multe scrieri de acest gen și tot el a presupus că două tablete descoperite la Susa (în Iranul de astăzi) pot fi coduri. Pe bucățile de argilă spartă se găsesc două coloane paralele, una conținînd cuneiforme reprezentînd numere în ordine crescîndă, iar cealaltă cuneiforme reprezentînd sunete. Din nefericire, pe fragmentele de argilă recuperate nu se găsesc și numere folosite în textele cifrate descoperite pînă în prezent. Dacă aceste bucăți de argilă au fost într-adevăr coduri, atunci sînt cele mai vechi coduri cunoscute din istoria omenirii.

Cultura ebraică a consemnat trei tipuri de transformare prin substituție. Astfel, în Vechiul Testament apare cuvîntul Sheshach în locul cuvîntului Babilon și Leb Kamai în loc de caldeeni.

Ambele transformări au rezultat din aplicarea unei substituții tradiționale de litere, în care prima literă a alfabetului ebraic era substituită cu ultima și viceversa, penultima o înlocuiește pe cea de a doua etc. De exemplu: $a = z$, $b = y$, $c = x$; ...$z = a$. Acest sistem de substituție se numea „atbash".

Un alt sistem tradițional de substituție este cel numit „albam" și constă din împărțirea în două a alfabetului ebraic și substituirea reciprocă a literelor. Astfel, prima literă din partea întîi a alfabetului era substituită cu prima literă din partea a doua a alfabetului și așa mai departe.

Se cunoaște și un al treilea sistem de substituție, mai complicat, în care literele sînt înlocuite cu cifre. Acest sistem s-a numit „atbabh" și constă din substituirea primelor nouă litere

cu cifre de la unu la nouă, în așa fel încît suma rezultată din adunarea cifrei înlocuitoare cu numărul care reprezenta locul literei în alfabet să fie zece. Așa se înlocuia prima literă cu nouă, a doua cu opt etc., iar restul literelor se înlocuiau cu cifre care, adunate cu numărul de ordine al literelor, dădeau rezultatul o sută. Acest sistem era însă foarte confuz datorită modului de organizare a alfabetului ebraic și a numerelor ebraice.

Homer povestește pentru prima oară de folosirea conștientă a scrierii secrete în Grecia antică reproducînd legenda lui Bellerophon. Anteia, soția regelui Proteus, s-a îndrăgostit de Bellerophon, dar acesta nu a plăcut-o. Regina, rănită în amorul propriu, s-a dus la rege și l-a mințit că Bellerophon a vrut să o siluiască. Înfuriat, Proteus l-a trimis pe Bellerophon cu o scrisoare la regele Liciei, cerîndu-i acestuia să-l omoare, dar Bellerophon, prin faptele sale, cîștigă respectul regelui lician, care îi dă jumătate din regat și fata de soție.

Homer nu ne spune cum a fost scrisă această scrisoare de nu a putut fi citită de Bellerophon, preferînd să creeze în jurul ei o atmosferă de mister.

Cîteva secole mai tîrziu, Herodot, în ale sale „Istorii", se ocupă special de cîteva metode de steganografie (nu încă criptografie). Astfel, povestește că un med bogat, vrînd să se răzbune pe regele său, care-l făcuse să-și mănînce propriul copil, a trimis o scrisoare cu informații secrete, ascunse în burta unui iepure vînat în pădure, regelui Persiei, Cyrus, ajutîndu-l pe acesta să cucerească Mezia.

Tot Herodot povestește că un nobil persan a transmis ginerelui său Aristagoras, din Milet, într-un mod bizar, un mesaj în care îl îndemna la revoltă. Astfel, el a ras un sclav, a scris pe pielea capului lui informațiile pe care le aștepta Aristagoras, l-a lăsat să-i crească părul, apoi l-a trimis în Milet.

Conform cu „Istoriile" lui Herodot, spartanii au fost informați că Xerxes voia să cucerească Grecia de către un grec din Persia, care a transmis informații pe o placă de lemn acoperită cu ceară.

Spartanii au fost primii care au stabilit un sistem de criptografie militară. Încă din secolul al V-lea î.e.n., ei foloseau „skytala", primul „mijloc tehnic" folosit în criptografie. Skytala era o bucată de lemn în jurul căreia se înfășura o fișie de papirus, piele sau pergament și apoi se scria mesajul de-a lungul bucății de lemn. Cînd se desfășura papirusul de pe skytală, apăreau o serie de litere dispersate, care nu aveau nici un sens, dar care, dacă materialul pe care se scrisese se înfășura pe o skytală de aceeași grosime, puteau fi citite.

Grecii au avut și alte realizări în domeniul criptografiei. Lumea datorează primele instrucțiuni privind securitatea comunicațiilor tot grecilor. Aceste instrucțiuni sînt cuprinse într-un capitol special din lucrarea lui Aeneas Tacticianul „Despre apărarea orașelor întărite". Pe lîngă instrucțiuni, se descriu și unele sisteme de cifrare. Astfel, într-un asemenea sistem se propunea înlocuirea vocalelor din textul clar cu puncte, iar consoanele rămîneau neschimbate. Se recomanda, de asemenea, folosirea unui disc, în care se găseau anumite găuri reprezentînd literele alfabetului grecesc. „Cifrorul" trebuia să treacă un fir de ață prin literele care constituiau mesajul. „Descifrarea" se făcea prin procesul invers, iar semnificația mesajului apărea de-abia în momentul în care se termina scoaterea firului de ață din găurile discului. Un alt sistem sugerat de Aeneas a fost folosit și de spionii germani din primul război mondial și, cu o mică modificare, și în cel de-al doilea război mondial. Este vorba de a însemna, printr-o înțepătură, literele care constituie mesajul secret dintr-o scrisoare, carte sau alt document scris. Germanii, în cel de-al doilea război mondial, foloseau cerneala simpatică pentru a însemna literele care formau mesajul secret.

Un alt grec, Polybius, a inventat un sistem de semnalizare care a fost ulterior adoptat pe scară largă ca metodă criptografică. El a aranjat literele alfabetului într-un pătrat și a numerotat rîndurile și coloanele.

În acest caz, fiecare literă putea fi reprezentată de două cifre — una care indica rîndul, iar cealaltă coloana în care se găsea litera respectivă. Polybius propunea ca aceste numere să fie transmise cu ajutorul torțelor — o torță în mîna dreaptă

și cinci în mîna stîngă însemnau litera *e* etc. Criptografii moderni au găsit cîteva caracteristici patratului lui Polybius, sau careului cum i se spune acum, și anume: conversiunea literelor în numere și divizarea unei unități în două părți manevrabile. Careul lui Polybius, pe care îl prezentăm mai jos, a fost foarte mult folosit drept bază pentru un număr extrem de mare de sisteme de cifru.

	1	2	3	4	5
1	a	b	c	d	e
2	f	g	h	ij	k
3	l	m	n	o	p
4	q	r	s	t	u
5	v	w	x	y	z

Cu toate acestea, nu se cunoaște dacă grecii au folosit pe scară mare cifrurile pe bază de substituție. Primele atestări despre folosirea lor sînt cuprinse în „Războaiele galice", lucrarea lui Iulius Cezar, unde se prezintă modul în care a fost transmis un mesaj, scris cu litere grecești, lui Cicero, aflat într-o cetate asediată.

Suetonius scrie că Cezar folosea un cifru în care fiecare literă din textul clar era înlocuită cu o literă decalată cu trei locuri, după următorul model :

text clar — a b c d e f g h i j k l m n o p q r s t u v w x y z
cifru — D E F G H I J K L M N O P Q R S T U V W X Y Z A B C

După acest sistem, orice alfabet de cifrare care conține o periodicitate standard se numește alfabet Cezar.

Din lucrările de istorie rezultă că scrierile secrete se foloseau destul de mult de către romani și se spune că un gramatician, Valerius Probus, a scris chiar un tratat despre scrierile secrete ale lui Cezar, dar, din păcate, cartea s-a pierdut.

Se pare că, oriunde cultura a atins un anumit nivel de dezvoltare, în mod spontan a apărut și criptografia. Multiple nevoi i-au determinat pe oameni să recurgă la scrierile ascunse. Ast-

fel, Yezidi, o sectă obscură din nordul Irakului, folosea, de teama represaliilor musulmanilor, scrierea secretă cînd își redacta cărțile sfinte. Diferite sisteme de substituție se găsesc în vechile culturi din Tailanda, Malaya, Nigeria și chiar în unele insule din Pacific.

În Europa, runele teutone și oghamele celte erau uneori criptate.

Toate sistemele de criptografie runică se bazau pe înlocuirea literelor prin semne ce indicau numărul grupului literei și numărul literei în cadrul grupului.

Oghamele s-au păstrat mai ales pe inscripțiile de pe pietrele funerare. Alfabetul acestor scrieri era format din cinci grupe de cîte cinci litere, reprezentate de una pînă la cinci linii pornind de la o linie orizontală. Pentru primul grup, liniile erau situate deasupra orizontalei, pentru al doilea dedesubtul acesteia, pentru al treilea perpendicular, pentru al patrulea oblic, iar al cincilea eterogen.

Metodele acestea de criptare sînt catalogate într-o compilație, „Cartea lui Ballymote".

O dată cu căderea Imperiului Roman, Europa alfabetului latin s-a prăbușit în întunericul Evului Mediu. Pămîntul pe care avea să se nască criptografia modernă uita artele și știința, iar din criptografie doar iscălitura anagramată a cîte unui călugăr plictisit mai pîlpîia ca o candelă în altarul bisericii, mai mult subliniind întunericul decît luminînd. În Evul Mediu, sistemele folosite pentru scrierea secretă erau foarte simple: cuvintele se scriau vertical sau de la coadă; în loc de vocale se puneau puncte, se foloseau alfabetele străine (grec, ebraic și armean) etc. Aproape o mie de ani criptologia civilizației apusene a stagnat.

Singurul om din Evul Mediu care a vorbit de criptografie, pe lîngă faptul că s-a folosit de ea, a fost Roger Bacon, iar cel mai vestit cărturar care a avut cunoștință de criptografie în acele vremuri a fost un vameș englez, astronom amator și scriitor de geniu, pe nume Geoffrey Chaucer. Într-o lucrare de astronomie „Tratatul despre astrologie", Chaucer include șase

pasaje criptate. Chaucer a substituit literele cu diferite semne făcute de el, punînd astfel bazele unui nou tip de scriere secretă.

În perioada aceasta însă, criptografia a căpătat o tentă de mister, fiind considerată o artă neagră, diavolească.

Scrierea secretă la arabi a apărut o dată cu interesul pentru literatură și gramatică, pentru rebus, epigrame, anagrame, ghicitori.

În anul 855, învățatul arab Abu Bakr Ahmad ben Ali ben Wahahiyya an-Nabati a inclus cîteva cifruri folosite de magie în cartea sa, „Cartea devotatului credincios care vrea să afle misterele scripturilor vechi". Apoi, criptografia a căpătat și o altă întrebuințare. Astfel, într-un manuscris despre arta militară se vorbește de un cifru cu ajutorul căruia se relata despre compoziția materialului inflamabil ce era aruncat în cetățile asediate. Sectele religioase extremiste cultivau criptografia ca un mijloc de ascundere a părerilor lor față de credincioșii ortodocși.

Statele arabe au folosit, totuși, puțin cifrurile și codurile, deși în istoria lui Abd al-Rahman Ibn Khaldun se spune că funcționarii fiscului și cei din birourile armatei foloseau în relațiile dintre ei un cod special. Astfel, literele alfabetului sau numele de oameni erau înlocuite cu nume de parfumuri, fructe, păsări, flori ori alte semne decît cele general cunoscute.

Cunoștințele arabilor în domeniul criptologiei au fost concentrate într-o secțiune specială a enciclopediei în 14 volume „Subh al-asha". Secțiunea despre criptologie intitulată „Cu privire la ascunderea mesajelor secrete în scrisori" are două părți, prima referindu-se la sisteme simbolice și aluzive, iar cealaltă la cerneluri simpatice și criptologie propriu-zisă.

Autorul acestei enciclopedii, Qualqashandi, își datorează informațiile scrierilor sale lui Ibn ad-Duraihim. Qualqashandi începe secțiunea despre criptologie explicînd de ce uneori este necesar să se asigure secretul unor mesaje și, după ce arată că se poate asigura secretul unor informații folosindu-se o limbă străină puțin cunoscută, el dă șapte sisteme de criptare :

1) O literă se înlocuieşte cu alta ; 2) criptologul poate scrie cuvîntul invers, de la coadă; 3) se poate schimba locul literelor din cuvintele care alcătuiesc mesajul; 4) se pot da literelor valorile lor numerice, după sistemul în care literele arabe sînt folosite ca cifre, scriind astfel cuvîntul cu ajutorul numerelor; 5) se poate înlocui fiecare literă a textului clar cu două litere a căror valoare numerică adunată să dea o sumă egală cu valoarea numerică a literei substituite; 6) fiecare literă poate fi substituită cu un nume de persoană sau ceva asemănător; 7) se pot folosi nume de ţări, fenomene cosmice, nume de fructe, flori, copaci pentru a substitui literele sau să se deseneze păsări sau alte fiinţe ori, pur şi simplu, să se inventeze simboluri speciale cu care să se înlocuiască literele.

Această listă cuprinde atît sisteme bazate pe substituţie, cît şi pe transpoziţie, iar sistemul „5" preconizează, pentru prima dată, folosirea mai multor elemente pentru substituirea unei litere.

Filologii arabi, mai ales gramaticienii din Basra, Kufa şi Bagdad, prin studierea Coranului au încercat, numărînd frecvenţa cuvintelor, să stabilească ordinea cronologică a versetelor din Coran.

Cu această ocazie, ei au observat că unele cuvinte au fost folosite mai des doar în ultima parte a acestuia şi le-au examinat din punct de vedere fonetic să vadă dacă erau arabe sau împrumuturi. Toate aceste studii au dus la generalizări despre compoziţia cuvintelor arabe şi astfel s-a ajuns la concluzia că sînt foarte puţine cuvinte, formate din mai mult de cinci litere, care să nu cuprindă lingualele *r*, *l* şi *n* sau labialele *f*, *b* şi *m*.

De asemenea, de mare importanţă pentru criptanaliză au fost descoperirile făcute cu ocazia întocmirii de dicţionare sau, mai bine-zis, a dezvoltării lexicografiei.

Cînd întocmeşte un dicţionar, lingvistul se loveşte întotdeauna de problema frecvenţei literelor şi a asocierilor de litere. Astfel, arabii au aflat foarte repede că cel mai rar întîlnită în arabă este litera *z*, iar cel mai des întîlnite sînt literele care alcătuiesc articolul hotărît *al*, adică *a* şi *l*. Se înţelege, deci,

de ce primul mare filolog al lumii, Al-Khalil, a scris o carte numită „Manualul limbii secrete". Lucrarea i-a fost inspirată de modul în care a reuşit să găsească soluţia unei criptograme scrisă în limba greacă şi care îi fusese trimisă pentru decriptare de către împăratul bizantin.

Întrebat cum a reuşit să decripteze scrisoarea, Al-Khalil a afirmat că primul lui gînd a fost că mesajul respectiv trebuia să înceapă cu „În numele lui Dumnezeu" sau ceva asemănător. Foarte curînd, prezumţia lui s-a dovedit justă.

Această afirmaţie, precum şi faptul că lui Al-Khalil i-a trebuit o lună să decripteze scrisoarea demonstrează că arabii nu formulaseră încă cele mai analitice tehnici ale criptanalizei, bazate pe frecvenţa literelor. Dar 600 de ani mai tîrziu, studiile lingvistice au ajutat un necunoscut să aplice observaţiile făcute şi în criptanaliză, căci Qualqashandi scrie că: „Ocazional, secretari pricepuţi, deşi nu cunosc codul, totuşi cunosc reguli care îi ajută, prin combinaţii, să rezolve enigme".

Qualqashandi vorbeşte, în continuare, despre modul în care se face criptanaliza unui text, făcînd iniţial afirmaţia că orice criptanalist trebuie să ştie în ce limbă e scris mesajul de decriptat. Afirmînd că araba este limba cel mai des folosită, îi descrie foarte amănunţit caracteristicile. Se dă, astfel, lista literelor care nu se întîlnesc niciodată împreună într-un cuvînt, a literelor care intră foarte rar în combinaţii sau combinaţii de litere care nu sînt posibile. Urmează apoi lista literelor în ordinea frecvenţei lor din versetele Coranului, făcîndu-se menţiunea că în alte texte frecvenţa poate fi diferită. După ce a făcut toate aceste precizări, Qualqashandi a scris :

„Cînd doriţi să găsiţi soluţia unui mesaj cifrat, începeţi prin a-i număra literele, apoi număraţi de cîte ori se repetă fiecare simbol în parte, notîndu-vă rezultatele. Dacă persoana care a scris mesajul a fost atît de vicleană încît a ascuns despărţirea cuvintelor între ele printr-un simbol, primul lucru care trebuie să-l faceţi este să-l identificaţi pe acesta. În acest scop luaţi al doilea simbol din mesaj şi consideraţi-l ca fiind semnul de despărţire, apoi căutaţi-l în tot mesajul, observînd dacă combinaţiile celorlalte semne ar putea forma cuvinte, ţinîndu-se seama

de observațiile făcute la început. Dacă nu se potrivește, luați următorul simbol și faceți aceeași operație. Dacă nici acesta nu se potrivește, luați pe următorul și așa mai departe, pînă cînd puteți afirma că ați descoperit semnul de despărțire a cuvintelor.

Următoarea operațiune este aceea de a vedea care semn se repetă cel mai mult și îl comparați cu lista frecvenței. Plecați de la prezumția că litera cea mai des întîlnită este *a*, iar următoarea *l*. Corectitudinea prezumției se confirmă prin faptul că, în majoritatea textelor, după *a* urmează *l*.

Apoi, primele cuvinte asupra cărora vă concentrați atenția sînt cele formate din două litere, folosind combinațiile cele mai des întîlnite, pînă cînd credeți că ați găsit o soluție sigură. Căutați simbolurile respective și scrieți echivalentul lor deasupra. Acordați apoi atenție cuvintelor formate din trei litere și procedați ca și în cazul cuvintelor formate din două litere, trecînd apoi la cuvintele compuse din patru, cinci și mai multe litere. Ori de cîte ori aveți vreo îndoială, scrieți una sub alta mai multe litere posibile pentru același simbol, pînă cînd, din alt cuvînt, se confirmă care este adevărata lui valoare".

După această explicație clară a modului în care trebuie abordat un text pentru decriptare, Qualqashandi exemplifică afirmațiile cu o soluție din Ibn ad-Duraihim.

Deși arabii au ajuns la asemenea culmi, nu se știe în ce măsură criptologia a influențat istoria lumii musulmane, dar se știe, în schimb, că și aceste cunoștințe au căzut în desuetudine și s-au pierdut. În anul 1600, o criptogramă a unui ambasador al Marocului la curtea reginei Elisabeta a Angliei a ajuns în mîinile unui alt arab, căruia i-au trebuit cincisprezece ani pînă să o decripteze, deși era vorba de un sistem de criptare foarte simplu. Acest fapt constituie dovada elocventă a pierderii uriașei moșteniri criptologice, ținîndu-se seama că Ibn ad-Duraihim decriptase un mesaj asemănător doar în cîteva ore !

Analiza frecvenței și combinațiilor de litere constituie principalul procedeu criptanalitic. Cunoașterea lui este esențială

pentru înțelegerea tuturor celorlalte tehnici de criptanaliză a substituțiilor. De aceea, consider că merită să mă opresc și să-l detaliez, luînd spre exemplificare o soluție în engleză a unei criptograme.

Criptanaliza se bazează pe faptul că literele unei limbi au o „personalitate" proprie. Unui observator neavizat, ele pot să-i apară ca soldații aliniați pentru inspecție, dar așa cum sergentul își cunoaște oamenii după trăsăturile caracteristice ale fiecăruia, tot așa și criptanalistul cunoaște fiecare literă a alfabetului. Deși într-o criptogramă acestea sînt deghizate, criptanalistul le observă acțiunile și idiosincrețiile, descoperindu-le identitatea. În substituția monoalfabetică obișnuită, sarcina criptanalistului e foarte simplă, deoarece fiecare literă, purtîndu-și masca de-a lungul întregului text, își trădează identitatea.

Ce va face criptanalistul dacă primește această criptogramă ?

GJXXN	GGOTZ	NUCOT	WMOHY
GINUG	JFNZV	QHYNG	NEAJF
FTUIN	ZANFG	NLNFU	TXNXU
TUCQG	OGOTH	JOHOA	TCJXK
GHHAF	NUZHY	NCUTW	JUWNA
HOGLN	FQZNG	OFUVC	NZJHT
OGHTN	ABNTO	TWGNT	HNTXN
TJUCE	AFHYN	GACJH	OATAE
JTKTA	MTXOB	YNFGO	
HYOTW	GOTHY	NAFZN	
FNEJC	INHYA	ZGAEU	
HYNUV	OCOHQ	UHCNU	
EHYNA	FOWOT	UCHNP	
AHNGG	NTHOU	CGJXY	
AEBUF	KNFYO	HHGIU	
IOCOH	UFOXO	BYNFG	

El începe prin a stabili frecvența fiecărei litere (de cîte ori e întîlnită în text) și vecinele ei (care sînt literele cu care vine

în contact și cîte dintre acestea sînt diferite). Frecvența criptogramei de mai sus este următoarea :

17	4	13	0	7	17	23	26	5	12	3	2	2
A	B	C	D	E	F	G	H	I	J	K	L	M
36	25	1	5	0	0	23	20	3	6	9	13	8
N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Un tabel conținînd frecvența într-un text în engleza obișnuită format din 200 de litere ar putea fi următorul :

	16	3	6	8	21	4	3	12	13	1	1	7	6
	A	B	C	D	E	F	G	H	I	J	K	L	M
Procentaj	8	1,5	3	4	13	2	1,5	6	6,5	0,5	0,5	3,5	3
	14	16	4	½	13	12	18	6	2	3	1	4	½
	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Procentaj	7	8	2	0,25	6,5	6	9	3	1	1,5	0,5	2	0,25

Dar nu este posibil să facem substituirea luînd, în mod mecanic, literele din criptogramă, în ordinea frecvenței și alăturîndu-le listei cu frecvența într-un text obișnuit.

În cazul nostru, cele două liste ar apărea așa :

text obișnuit	e	t	a	o	n	i	r	s	h	d	l	u	c	m
criptograma	N	H	O	G	T	U	A	F	C	Y	J	X	Z	E
text obișnuit	p	f	y	w	g	b	v	j	k	q	x	z		
criptograma	W	I	Q	B	X	V	L	M	P					

Substituția mecanică a celor două texte ar da un text de tipul: olunevoanceihanpjatd, fără nici un sens. Nu trebuie să surprindă pe nimeni acest lucru, deoarece cele două liste se bazează pe texte *diferite*, cuprinzînd cuvinte *diferite*, formate din litere *diferite*. Totuși, frecvența lor se schimbă foarte puțin, neîndepărtîndu-se prea mult de locul lor obișnuit de pe lista frecvenței. Orice text ar fi, literele *e, t, a, o, n, i, r, s* și *h* vor forma grupuri de litere cel mai des întîlnite; urmează apoi grupul literelor *d, l, u, c* și *m* întîlnite destul de frecvent, grupul

literelor *p, f, y, w, g, b* găsite mai rar și ultimul grup, cel al literelor *j, k, q, x* și *z*, care se întîlnesc foarte rar.

Dacă un criptanalist a reușit să identifice, într-un fel sau altul, unele litere dintr-un text cifrat, celelalte le descoperă ghicindu-le, ca în textul de mai jos :

GJXXNGGOTZNUCOTWMOH
    e   in ea in   it

YJTKTAMTXOBYNFGOGINUGJFN
h n no n i he i ea e

ZVQHYNGNEAJFHYOTWGOTHYNAFZ
  the e o thin intheo

NFTUINZANFGNLNFUTXNXUFNEJCINHYA
e na e oe e e ane a e etho

ZGAE
 o

UTUCQGOGOTHJOHOATCJXKHYNUVOCOHQUH
a na i int ition   thea i it at

CNUGHHAFNUZHY
 ea tto ea th

Aproape de începutul textului, se găsește combinația *ith*. Aceste litere pot face parte din cuvîntul *with*.

Nici un criptanalist, dacă ar fi întrebat, n-ar avea cum să vă dovedească că presupunerea lui e corectă. De acum încolo totul se rezumă la ghicit, operațiune ghidată doar de elasticele legi ale probabilității. Presupunerile succesive vor confirma supozițiile inițiale sau le vor infirma, deși fiecare presupunere pornește de la aceeași bază extrem de șubredă. În cele din urmă însă, consistența rezultatului final este atît de probabilă încît validitatea soluției devine certitudine. Se știe că criptanalistul care caută dovezi absolute pentru fiecare presupunere pe care o face nu va găsi niciodată soluția unei criptograme. Dar să revenim. În cazul nostru se pare că *with* este cuvîntul care se

ascunde sub aceste litere, ceea ce ar însemna că $M = W$. Se face înlocuirea lui în criptogramă cu scopul de a vedea dacă nu cumva nu ne sugerează și alte cuvinte. Zece litere în continuare formează secvența *with n-nown...* care ne duce la deducția că ar putea fi vorba de expresia: *with unknown*. Secvența din textul clar — *int-ition* — ne dă prilejul să verificăm dacă $j = u$ și vom vedea că așa este, deoarece apare cuvîntul *intuition*. Noile litere clare care au apărut sînt inserate în text și ele ne ajută să identificăm și alte litere. Acest proces de reconstrucție a textului clar, probabil cel mai ușor lucru și cel mai amuzant din criptanaliză, este numit „anagramare". El poate fi accelerat de o reconstrucție paralelă și anume aceea a cheii de cifrare. Dacă literele din textul cifrat sînt scrise sub un alfabet normal, acest aranjament ne furnizează, de multe ori, și alți echivalenți. În cazul de față, situația se prezintă astfel :

Alfabet clar	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Alfabet cifrat	u				n			y	o		k			t	a					h	j		m			

Deoarece este greu de ținut minte un șir de 26 de litere nelegate între ele care constituie întreaga serie de echivalente, alfabetele cifrate sînt deseori bazate pe un singur cuvînt ușor de memorat. Sînt posibile diferite variante, dar cea mai simplă este de a folosi o *cheie*, omițînd literele care se repetă, apoi înșirînd în ordinea normală restul literelor din alfabet. Astfel, alfabetul de cifrat ar fi următorul, dacă cheia este cuvîntul CHIMPANZEE :

Alfabet clar	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Alfabet cifrat	C	H	I	M	P	A	N	Z	E	B	D	F	G	J	K	L	O	Q	R	S	T	U	V	W	X	Y

Porțiunea din alfabetul cifrat care urmează după cheie, conține mai multe secvențe alfabetice. Deseori, criptanalistul poate completa anumite secvențe care au fost parțial descoperite și astfel să identifice și alți echivalenți. De exemplu, dacă observă secvența $QR - TU$, nu-i nevoie de prea mult efort pentru a-și da seama că litera care lipsește este *s*. Asemenea secvențe sar în ochi în cazul alfabetului parțial decriptat din

criptogramă: *HJ — M*. Doar două litere pot să intre în acest spațiu: *K* și *L*. Dar *k* a fost identificat în cuvîntul *unknown*, deci $L = V$. Același lucru îl poate ajuta pe criptanalist să verifice dacă *F* și *G* sînt *r* și *s*. Dacă $F = s$ și $G = r$, ordinea în alfabet ar apărea ca *sr*, deci nu e bine și acum sîntem siguri că $F = r$ și $G = s$. Alfabetul de cifrat ne asigură, de asemenea, și o serie de indicii pentru echivalența din textul clar. Așa, de exemplu, $u = a$ în alfabet. Deci, în cazul în care criptanalistul observă un *V* în criptogramă, el încearcă să vadă dacă *V* nu este cumva *b* și aceasta datorită secvențelor *UV* și *ab*. În cazul de față, această presupunere se dovedește justă. Cu noile descoperiri inserate în primele două rînduri, soluția, putem spune fără frică, a fost găsită :

G	J	X	X	N	G	G	O	T	Z	N	U	C	O	T	W	M	O	H		
s	u			e	s	s	i	n		e	a		i	n		w	i	t		
Y	J	T	K	T	A	M	T	X	O	B	Y	N	F	G	O	G	I	N	U	G
h	u	n	k	n	o	w	n		i		h	e	r	s	i	s		e	a	s
J	F	N	Z	V	Q	H	Y	N	G	N	E	A	J	F	H	Y	O	T	W	
u	r	e		b		t	h	e	s	e		o	u	r	t	h	i	n		

Cei doi *XX* pot fi cei doi *cc* din *success*, apoi *B* trebuie să fie *p* din *ciphers*; *E* trebuie să fie *f* din *four*; $W = g$ din *things* sau din *-ing* și așa mai departe. Textul clar, inserînd și semnele de punctuație, ar fi :

„Success in dealing with unknown ciphers is measured by the four things in order named: perseverance, careful methods of analysis, intuition, luck. The ability at least to read the language of the original text is very desirable but not essential" [1].

În situația de față, cheia folosită la cifrare a fost NEW YORK CITY.

---

[1] În limba română : „Succesul în rezolvarea cifrurilor necunoscute este asigurat de următoarele patru lucruri enumerate în ordine : perseverență, metode de analiză, alese cu grijă, intuiție, noroc. Deprinderea de a citi în limba în care este scris textul original e de dorit într-un grad foarte înalt, dar nu este esențială".

În cazul substituțiilor monoalfabetice, de multe ori soluția se poate afla încercînd identificarea conjuncțiilor și articolelor, căutînd să ghicim anumite cuvinte care se repetă mai des (*W X Y Z Y* poate fi *There*) sau comparînd cuvinte scurte (*H X, X H, X L, P L* și *P X* pot fi *on, no, of, if* și *in*). Aceasta numai dacă se păstrează spațiul dintre cuvinte. Cunoașterea caracteristicilor textului clar stă la baza soluționării unor cifruri și coduri mult mai complexe. Natural, soluția criptogramelor scurte este mult mai greu de găsit decît a celor lungi, care conțin destul material pentru a ne confirma presupunerile.

Pentru problemele mai dificile, experții sfătuiesc pe novici : 1) să facă tabele de contact, deoarece în felul acesta identificările apar mult mai repede; 2) cînd nu este evident nici un fel de text clar sau cuvînt, să încerce *ceva* și să vadă ce iese, căci chiar dacă prezumția a fost greșită, numărul de posibilități se reduce. Nici o criptogramă n-a fost rezolvată doar privind-o. Mai remarcăm că și în cazul în care literele alfabetului sînt înlocuite cu cifre, se procedează în același fel. Schimbarea măștilor nu schimbă caracteristicile limbii ce se ascund după ele.

RIDICAREA VESTULUI

De îndată ce a ieșit din întunericul Evului Mediu, Europa apuseană a început să folosească criptologia în documentele diplomatice și politice, dar scrierea secretă din acea vreme era în stare embrionară, ca de altfel toate celelalte elemente ale civilizației care, peste secole, vor domina lumea. Sistemele folosite în scrierea secretă erau rudimentare chiar și în cadrul bisericii, pe atunci cea mai mare și mai influentă putere, dar criptologia, începînd cu această perioadă, n-a mai cunoscut regrese, ci s-a dezvoltat continuu sub cele două forme de bază cunoscute și astăzi: coduri și cifruri.

Substituțiile în coduri își au originea atît în abrevieri cît și în epitetele și figurile de stil folosite de oracole și vrăjitori (formule magice menite pe jumătate să sublinieze, pe jumătate să ascundă adevăratul înțeles al vrăjilor).

Cel mai vechi document criptografic, aflat în arhivele Vaticanului, include substituții provenind din ambele izvoare. Este vorba de o listă pe care sînt trecuți guelfii care-l susțineau pe papă și ghibelinii care-l susțineau pe împăratul german. În acest document, guelfii erau numiți „egipteni", iar ghibelinii „copiii lui Israel". Mai tîrziu, după vreo zece ani, pe o bucată de hîrtie a fost scris primul cod modern. În acest cod, bazat pe substituție, o literă ține locul unui cuvînt. Astfel : *a* = rege, *d* = papa, *s* = Marescallus și așa mai departe.

În ce privește cifrurile, acestea au fost folosite destul de des. Astfel, vocalele erau înlocuite cu puncte sau cruci. Arhi-

episcopul Neapolului, Petro di Orazie, folosea în mod regulat acest procedeu în corespondenţa lui cu curia papală sau cu alţi cardinali.

Papa de la Avignon, Clement al VII-lea, l-a folosit pe Gabrieli di Lavinde ca cifror, iar acesta a compilat o serie de chei pentru 24 din corespondenţii săi. Această compilaţie, pe lîngă o substituţie simplă şi un număr de cuvinte înlocuite cu două litere, cuprindea şi elemente de cod. Aşa a apărut primul nomenclator care unea substituţia alfabetică de litere cu lista de cod (echivalentele cuvintelor, silabelor şi ale numelor proprii).

Dacă primele alfabete de substituţie conţineau un singur substitut pentru fiecare literă, foarte curînd au apărut cifruri în care mai multe cifre reprezentau aceeaşi literă. Cu toate acestea, criptografia progresa încet. Dezvoltarea acesteia a fost rezultatul direct al dezvoltării diplomaţiei moderne. Ambasadorii trimiteau acasă, în mod regulat, rapoarte şi, pentru a-şi ascunde comunicările secrete, au fost nevoiţi să-şi cifreze mesajele. Fiind o sursă de a cunoaşte atît activitatea acestora cît şi intenţiile statelor pe care le reprezentau, s-a ivit necesitatea criptanalizei.

Pe la sfîrşitul secolului al XVI-lea, criptologia devenise atît de importantă încît multe state şi-au asigurat un personal care se ocupa cu elaborarea de cifruri, cu cifrarea şi descifrarea mesajelor, cu soluţionarea scrisurilor cifrate.

Veneţia a fost oraşul care a deţinut în acea perioadă întîietatea în acest domeniu, datorită mai ales lui Giovanni Soro, care a fost poate primul mare criptanalist al Occidentului. Atît de mare era faima lui Soro, care descifrase o scrisoare a lui Mark Colonna, comandantul armatei germane aflată în Italia, încît curia papală îi trimitea pentru soluţionare mesajele care nu puteau fi descifrate la Roma. În activitatea sa, Soro a soluţionat mesaje criptate aparţinînd lui Carol al V-lea, ducelui de Ferrara şi multe altele. Dar Veneţia, deşi a făcut mari eforturi, n-a putut deţine supremaţia în acest domeniu, căci şi în alte oraşe şi state italiene criptanaliza s-a dezvoltat rapid. Astfel, la Florenţa, Pirrho Musefili a soluţionat zeci de mesaje cifrate, a întocmit nomenclatoare de cifruri pentru regele Franţei şi cardinalul di Mendoze. Printre „clienţii" lui Musefili se numărau regele Angliei, ducele de Alba şi alte personaje ilustre ale epocii. Succesorul lui Musefili, Camillo Giusti, s-a bucurat de o reputaţie şi mai mare, mai ales după ce s-a pus în slujba familiei di Medici.

Şi în alte ţări, nu numai în Italia, criptologia s-a dezvoltat foarte mult în acea perioadă. Astfel, la curtea regelui Franţei, Philibert Babou se ocupa cu decriptarea mesajelor interceptate de supuşii credincioşi ai regelui.

Nici englezii nu se dădeau în lături cînd era vorba să intercepteze şi să afle ce scriau ambasadorii acreditaţi la Londra.

În peninsula Iberică, cunoştinţele criptologice ale timpului au pătruns cu multă repeziciune încă de pe vremea cînd maurii erau alungaţi din Catalonia de către Ferdinand şi Isabela. Dezvoltarea criptologiei în această parte a Europei a cunoscut un curs ascendent, ajungîndu-se ca nomenclatorul de cifruri şi coduri folosit de Filip al II-lea să fie unul din cele mai perfecţionate nomenclatoare ale vremii. Regele Spaniei folosea cifrurile mai ales în corespondenţa sa cu Liga catolică din Franţa, care se opunea urcării pe tronul Franţei a regelui Henric al IV-lea. Cu toate măsurile luate, o parte din această corespondenţă a căzut în mîinile regelui Henric al IV-lea, la curtea căruia, un oarecare François Viète, avocat, ajuns pînă la înalta funcţie de consilier particular al regelui, îşi petrecea timpul liber rezolvînd probleme de matematică. Din amuzament, Viète a încercat să soluţioneze un mesaj cifrat şi a reuşit, fapt care l-a determinat pe rege să-i ceară descifrarea corespondenţei interceptate. Viète a spart cifrul folosit de regele Spaniei şi a soluţionat o serie de criptograme, deşi de multe ori cu întîrziere.

Cifrurile şi codurile spaniole au mai fost atacate şi de Philip von Marnix, mîna dreaptă a lui Filip de Orania şi compozitorul imnului naţional olandez. Succesele criptanalistului Marnix au contribuit la cucerirea independenţei naţionale de

către Olanda, demonstrînd lumii importanța criptologiei în făurirea istoriei.

Printre cei mai buni criptologi ai timpului se numărau mai ales cei care lucrau pentru papă. În serviciul papei s-a înființat chiar un post de secretar-cifror. După 1580, acest post a intrat în posesia unei familii de criptologi care au impulsionat dezvoltarea criptologiei în ansamblul ei.

Este vorba de familia Argenti. Giovanni Batista Argenti a intrat în serviciul papal ca secretar al lui Antonio Elio, care l-a învățat meseria de criptolog. Nepotul lui Giovanni Argenti, Matteo Argenti, a învățat și el criptologie. El a făcut chiar și un manual de criptologie, în care a concentrat tot ceea ce realizase mai bun Renașterea în acest domeniu.

Cei din familia Argenti au fost primii care au folosit un cuvînt drept cheie pentru întocmirea unor alfabete cifrate. Procedeul este următorul : se scrie cheia, omițîndu-se literele care se repetă, apoi se completează șirul de litere cu restul alfabetului după modelul de mai jos :

P	I	E	T	R	O	a	b	c	d	f	g	h	l	m	n	q	s	u	z
10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29

Cunoscînd că secvența *qu* din textele clare este invariabilă și ajută la identificarea ambelor litere, Argenti a substituit-o cu o singură cifră. De asemenea, deoarece majoritatea literelor duble din cuvintele italiene sînt consoane, în textul cifrat s-a renunțat la una dintre acestea. Astfel, în loc de *sigillo* din textul clar, în textul cifrat se scria *sigilo*. Pentru a îngreuia descifrarea, cei doi Argenti foloseau nulele de la 3 la 8 pe un rînd.

Eliminînd despărțirea în cuvinte, punctuația și accentele, care pînă atunci se făceau în clar, ei au conferit textului cifrat o rezistență superioară.

În același timp, foloseau atît numere formate dintr-o singură cifră cît și numere formate din două cifre, avînd grijă ca numerele compuse dintr-o singură cifră să înlocuiască litere

cu frecvență mare, pentru a nu atrage atenția prin raritatea lor. Iată un astfel de cifru folosit de Matteo Argenti :

a	b	c	d	e	f	g	h	i	l	m	n	o	p	q	r	s	t	u	z
1	86	02	20	62	22	06	60	3	24	26	84	9	66	68	28	42	80	04	88

et	con	non	che	nub
08	64	00	44	5,7

Foloseau, de asemenea, foarte mult polifonele — simboluri care aveau două sau chiar trei înțelesuri — alese însă în așa fel încît să nu îngreuieze decriptarea de către destinatar. Matteo Argenti folosea, de asemenea, cifruri pe care le adapta în funcție de alfabetul limbii în care era scris textul de cifrat, neavînd un cifru standard, universal valabil pentru toate limbile.

Toate aceste succese duceau la nașterea unei științe evoluate, în conformitate cu progresul realizat de cunoașterea umană.

Părintele criptologiei apusene a fost Leon Battista Alberti, primul dintr-un grup de oameni care au inventat, element după element, un sistem de cifru căruia îi aparțin majoritatea cifrurilor folosite astăzi. Este vorba de substituția polialfabetică. După cum arată și numele, avem de-a face cu două sau mai multe alfabete-cifru. Deoarece mai multe alfabete folosesc aceleași simboluri (în special litere) pentru cifrare, un anumit simbol poate reprezenta diferite litere din același text clar, în funcție de alfabetul care a fost folosit. În mod sigur, acest lucru îl va dezorienta pe criptanalist. Se poate întîmpla însă ca și criptograful să facă anumite confuzii, nemaiștiind care alfabet a fost folosit și, pentru a se evita acest lucru, se stabilesc anumite reguli și convenții.

Apariția substituției polialfabetice a însemnat un uriaș pas înainte în criptologie, dar a fost nevoie de peste 400 de ani pînă cînd aceasta s-a impus în criptografia politică. În secolul XX, folosirea ei a atins un înalt grad de complexitate, ceea ce asigură textelor cifrate o rezistență extraordinară.

Cei care au inventat acest sistem de cifrare au fost amatorii, deoarece profesioniştii, care îi întreceau pe amatori în criptanaliză, se concentrau asupra problemelor curente şi asupra sistemelor care se foloseau pe vremea aceea, dar care astăzi sînt depăşite. Amatorii, nelegaţi de astfel de probleme, făceau mai mult teorie, iar ideile a patru asemenea amatori — un arhitect, un cleric, un curtean şi un naturalist — au prins aripi.

Arhitectul a fost Alberti, care, la fel ca şi Leonardo da Vinci, întruchipa omul universal al Renaşterii. La rugămintea secretarului pontifical Leonardo Dato, Alberti a studiat şi a scris un eseu despre criptologie. După ce a reconstituit modul de descifrare a textelor criptate, a trecut la căutarea unor procedee de criptare care să reziste criptanaliştilor. Apoi a analizat pe rînd diferitele sisteme de cifrare : substituţii, transpoziţii de litere, punctarea literelor care constituiau un mesaj secret ascuns în interiorul unei scrisori, folosirea cernelurilor simpatice etc. În eseul său a prezentat şi un cifru făcut de el, despre care, la fel ca toţi criptologii, spunea că nu poate fi spart. Este vorba de discul de cifrat, care a ajutat la fundamentarea polialfabetismului. Cu această invenţie, Occidentul a preluat hegemonia lumii în probleme de criptologie şi n-a mai cedat-o niciodată.

Acum să-i dăm cuvîntul lui Alberti pentru a-şi prezenta invenţia :

„Am făcut două discuri rotunde din plăci de aramă. Pe cel mare l-am numit stator, iar pe cel mic rotor. Diametrul statorului este cu 1/9 mai mare decît cel al rotorului. Apoi am împărţit circumferinţa fiecărui disc în 24 de părţi egale şi spaţiile rezultate le-am numit celule. În celulele discului mai mare am scris literele mari ale alfabetului, omiţîndu-le pe *H*, *K* şi *Y*, deoarece nu sînt necesare. Asta a însemnat 20 de litere, deoarece *J*, *U* şi *W* nu făceau parte din alfabetul conceput de mine, iar în spaţiile goale am scris cifrele 1, 2, 3 şi 4. În fiecare din cele 24 celule ale rotorului am înscris o literă mică, dar nu în ordine alfabetică, cum este cazul cu statorul, ci la întîmplare. Toate cele 24 de celule au fost umplute, deoarece alfabetul latin are 24 de litere, printre care şi *et*. După ce am făcut completările respective, am aşezat rotorul peste stator, iar prin centru am înfipt un ac pe care se învîrtea rotorul".

Procedeul de lucru este următorul. Corespondenţii trebuie să aibă discuri identice şi să cadă de acord asupra unei litere index de pe rotor. Ca să execute cifrarea, expeditorul fixează această literă în dreptul oricărei litere de pe stator, avînd însă grijă ca aceasta să apară prima în textul cifrat. Alberti dă exemplul cu litera *K* în dreptul lui *B*. După aceasta, toate literele de pe rotor, care formează cuvintele din mesaj, sînt înlocuite cu cele de pe stator, aflate în dreptul lor. Pînă aici nimic deosebit, dar cu următoarea frază Alberti a deschis drumul criptologiei moderne :

„După ce am cifrat trei sau patru cuvinte, schimb poziţia indexului în dreptul lui *d*. Din acest moment, *K* nu mai este echivalent cu *B*, ci cu *d*, iar toate celelalte litere vor primi noi echivalenţi".

Fiecare nouă mişcare a rotorului înseamnă un nou cifru, în care atît literele textului clar cît şi echivalenţii lor sînt schimbaţi unul faţă de altul. În cazul de faţă, există exact atîtea cifruri cîte poziţii are discul. Discul lui Alberti a fost primul cifru polialfabetic din istoria criptologiei.

Acestei realizări, Alberti i-a adăugat o alta tot atît de remarcabilă : codul cifrat. Vorbind şi de această invenţie, avem explicaţia de ce Alberti a trecut pe discul exterior numerele de la 1 la 4. Într-un tabel, el a făcut permutări din aceste cifre, luate cîte două, cîte trei şi cîte patru, obţinînd 336 de numere, între 11 şi 4444.

În tabelul respectiv, în dreptul fiecărei cifre, se trecea o frază, o expresie sau un cuvînt. De exemplu, în dreptul lui 12 se scria : „Am pregătit corăbiile promise şi trupele s-au îmbarcat avînd şi hrana necesară". Aceste liste de cod nu se schimbau, dar cifrele rezultate în urma codificării erau cifrate cu ajutorul discului, ca şi cum ar fi fost litere simple. Operaţia ducea la schimbarea reprezentării codificate. Astfel, 341 = pază era o dată *mrp*, iar altă dată *fco*. Această invenţie a fost deose-

bit de valoroasă, dar au trecut 400 de ani pînă cînd marile puteri au început să o folosească.

În 1516, la Wurzburg, murea abatele mănăstirii, Johannes Trithemius, o minte iscoditoare, care lăsa în urma lui un manuscris cu titlul „Poligrafia". Urmaşul său la conducerea mănăstirii i-a publicat lucrarea, fiind astfel primul editor al unei lucrări de criptologie tipărite. Concepută din şase cărţi, lucrarea cuprinde coloane de cuvinte tipărite în alfabetul gotic folosit de Trithemius în sistemul său criptografic. În prima carte, 384 coloane de cuvinte latineşti, cîte două pe fiecare pagină, cuprind, criptat, vestitul Ave Maria. Este cea mai cunoscută invenţie a lui Trithemius. El a selectat în aşa fel cuvintele, echivalenţii literelor fiind luaţi din tabele consecutive, încît, în textul criptat, acestea au căpătat forma unei rugăciuni inocente. Astfel, cuvîntul *abate* este criptat ca fiind deus clementissimus regeus aevum infinivet. Celelalte cărţi cuprind sisteme de cifru asemănătoare, care, uneori, capătă o tentă de formule magice.

Cartea a cincea, însă, reprezintă contribuţia adusă de abatele Trithemius la dezvoltarea polialfabetismului. În această carte apare pentru prima dată tabelul pătrat sau tabloul. Acesta este forma elementară a substituţiei polialfabetice, deoarece prezintă dintr-o dată toate alfabetele de cifrat dintr-un anumit sistem. Tabloul este compus din şiruri de alfabete de cifrat puse în ordine unul sub altul, astfel încît fiecare şir oferă alţi echivalenţi pentru literele din alfabetul clar aflat pe primul rînd din tablou.

Cel mai simplu tablou este acela care foloseşte, ca alfabet de cifru, alfabetul normal în diferite poziţii. Dăm spre exemplificare cîteva rînduri din tabloul numit şi Tabula recta al lui Trithemius :

Trithemius a folosit acest tablou pentru cifrarea polialfabetică în cel mai simplu mod posibil. El cifra prima literă din textul clar, folosind primul alfabet, a doua, folosind al doilea, şi aşa mai departe. În felul acesta, un text latinesc începînd cu Hunc Caveto virum... devenea HXPF GFBMCZ FUEIB... În

cazul de faţă, el schimba alfabetul textului clar după prima grupă de 24 de litere, dar, de cele mai multe ori, folosea acelaşi alfabet pentru tot textul.

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	x	y	z	w
b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	x	y	z	w	a
c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	x	y	z	w	a	b
d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	x	y	z	w	a	b	c
.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
z	w	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	x	y
w	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	x	y	z

Marele avantaj faţă de invenţia lui Alberti este acela că un nou alfabet de cifrat este folosit pentru fiecare literă. Alberti schimba alfabetul după fiecare patru litere, iar rezultatele puteau să dea în vileag cuvinte de tipul lui papa sau atac, existînd şanse ca criptanalistul să descopere mecanismul şi să dezvăluie înţelesul criptogramei. Noul sistem exclude această posibilitate.

Sistemul de cifrare elaborat de Trithemius este în acelaşi timp şi primul exemplu de cheie progresivă, în care alfabetele folosite sînt scoase din uz înainte de a se fi repetat. Maşinile moderne de cifrat folosesc deseori asemenea chei, dar evită principalele defecte ale sistemului lui Trithemius, şi anume : periodicitatea alfabetelor şi ordinea rigidă a folosirii lor.

Trithemius a avut o influenţă deosebită în criptologie, datorită mai ales autorităţii pe care o conferă textul tipărit, iar *tabloul* său a devenit clasic pentru întreaga criptologie.

Dacă despre primii doi, care au contribuit la dezvoltarea criptografiei pe baza polialfabetismului, istoria ne furnizează date bogate, despre cel de-al treilea se ştie doar că era nobil din Brescia, pe nume Giovan Batista Belaso, că a făcut parte din suita unui cardinal, iar în 1553 a publicat o cărţulie cu titlul „La cifra". În această cărţulie, signor Giovan Batista Belaso propunea folosirea unei chei literare uşor de ţinut minte şi de schimbat pentru cifrurile polialfabetice. Belaso numea această cheie contrasemn şi spunea că „poate fi formată din

cuvinte din limbile italiană sau latină sau din orice altă limbă. Ea poate conţine două sau mai multe cuvinte, după dorinţa fiecăruia. Luăm textul pe care dorim să-l cifrăm şi-l punem pe hîrtie, scriind cuvintele nu prea aproape între ele. Apoi, deasupra fiecărei litere, scriem o literă din contrasemnul ales de noi. Să luăm, drept exemplu, cazul în care contrasemnul nostru ar fi versetul Virtuti omnia parent şi să spunem că ceea ce noi dorim să cifrăm este textul : Larmata Turchesca partira a cinque di Luglio. Le vom orîndui pe hîrtie în felul următor :

VIRTUTI OMNIA PARENT VIRTUTI OMNIA PARENT VI
larmata turch escapa rtiraac inquc dilugl io

Litera din cheie indică alfabetul din tablou, care urmează să fie folosit pentru cifrarea literei clare. Astfel, *l* urmează să fie cifrat cu litera corespunzătoare din alfabetul *V*, *a* cu litera corespunzătoare din alfabetul *I*. Sistemul permite o mare flexibilitate, nemaifiind nevoie ca toate mesajele să fie cifrate cu unul din cele relativ puţine alfabete de cifrat.

Acest sistem a prins repede, iar invenţia lui Belaso a pus bazele aranjamentelor extrem de complexe de astăzi cînd, pentru acelaşi text, se folosesc mai multe chei, care se schimbă la intervale neregulate.

Belaso, ca şi Trithemius, a folosit alfabete de cifrat standard, aşa că a rămas în seama unui naturalist să reînvie alfabetele mixte ale lui Alberti şi să închege, din invenţiile celor trei, conceptul modern de substituţie polialfabetică.

Naturalistul, primul care a trecut la cunoaşterea naturii prin experimente, se numea Giovanni Battista Porta şi a fost unul din cei mai de seamă oameni de ştiinţă de pe timpul Renaşterii.

În istoria criptologiei a rămas datorită unei cărţi, De Furtivis Literarum Notis, publicată pe cînd avea 28 de ani.

Marea calitate a acestei lucrări este perspectiva pe care autorul ei o deschide criptologiei. Cele patru capitole mari ale lucrării tratează criptografia antică, cifrurile moderne, criptanaliza şi prezintă o listă de particularităţi care ajută la soluţionarea criptogramelor.

Printre cifrurile prezentate se întîlneşte şi primul cifru digrafic, în care două litere erau reprezentate de un singur simbol.

El clasifica metodele de cifrare în trei sisteme : 1) schimbarea ordinii literelor (transpoziţia); 2) a formei literelor (substituţie prin simbol); 3) a valorii literelor (substituţie prin litere aparţinînd altui alfabet). Aceasta a fost prima clasificare a cifrurilor în cifruri de transpoziţie şi substituţie.

El sfătuia, de asemenea, pe cifrori să folosească în textul clar cît mai multe sinonime, iar unele cuvinte să fie ortografiate cu bunăştiinţă greşit, pentru a îngreuia soluţionarea criptogramelor.

În carte sînt mai multe discuri şi este explicat modul în care acestea pot fi transformate în tablouri, descriind, de asemenea, şi modul în care se poate soluţiona un cifru monoalfabetic, atunci cînd criptograma nu conţine despărţirea în cuvinte sau cînd despărţirea e făcută arbitrar. Dar, poate, cea mai de seamă contribuţie a sa, pe această linie, este încercarea de a soluţiona cifruri polialfabetice şi de a pune la punct metoda cunoscută azi sub numele de metoda cuvîntului probabil. Astfel, scoţînd în relief care este diferenţa dintre această metodă şi analiză lingvistică, spunea : „Cînd se cunoaşte, în general, despre ce este vorba în mesaj, criptanalistul poate încerca să ghicească cuvintele din criptogramă, analizînd fiecare cuvînt (număr de litere, ordinea şi comparîndu-le cu supoziţiile sale). În fiecare domeniu există un număr de cuvinte mai frecvente. Astfel, dacă este vorba de război, cuvinte ca soldat, comandant, general, tabără, armată, arme, a lupta etc. se întîlnesc foarte des. În felul acesta, se poate decripta un text, fără a se face analiza lingvistică a textului cifrat".

Porta, adoptînd singura poziţie care asigură succesul în criptanaliză — a refuzat să creadă în invincibilitatea cifrurilor polialfabetice — a reuşit să soluţioneze cîteva asemenea cifruri, reuşită cu atît mai remarcabilă, cu cît această problemă

era considerată de criptologia renascentistă ca fiind de nerezolvat.

Primul cifru polialfabetic pe care l-a soluţionat şi care a fost realizat cu ajutorul unui disc învîrtit în sensul acelor ceasornicului, după cifrarea fiecărei litere, avea un caracter progresiv. Porta a observat că, în cazul în care trei litere apar în ordine alfabetică, în cuvîntul din textul clar (de exemplu, def din deficio sau stu din studium) şi discul se mişcă progresiv cu un singur spaţiu. Astfel, în mod succesiv, în faţa fiecăreia din cele trei litere va apărea acelaşi simbol, rezultînd o repetare de trei ori a lui. Folosindu-se de această constatare, Porta a soluţionat o criptogramă şi a reconstruit alfabetul de cifrat. În cazul celei de-a doua soluţii, Porta şi-a schimbat metoda.

De data aceasta repetarea de trei ori a unui simbol i-a semnalat faptul că fusese folosită o cheie care conţinea un cuvînt avînd în compoziţia sa trei litere aşezate în ordine alfabetică şi că textul clar conţinea trei litere aşezate în ordine inversă faţă de cele din alfabet. În timp ce se ocupa de această observaţie a sa şi pe cînd scria că „întrucît sînt 51 de litere între primii trei M şi aceleaşi trei litere repetate în cel de-al treisprezecelea cuvînt, am ajuns la concluzia că cheia se repetase de trei ori şi era formată din 17 litere", a fost pe punctul de a descoperi metoda de decriptare a cifrurilor polialfabetice, dar el n-a dat atenţie descoperirii sale şi, mai mult de 300 de ani, cifrurile polialfabetice au fost considerate ca fiind inviolabile.

Deci, contribuţia lui Porta la dezvoltarea criptologiei constă în închegarea unui concept mai unitar asupra sistemului de cifrare polialfabetică.

Deşi Porta reuşise să închege un sistem de cifrare bazat pe cifrul polialfabetic, acestuia i se mai puteau aduce îmbunătăţiri. Doi oameni care au trăit în secolul al XVI-lea au acţionat asupra modului de folosire a cheii lui Belaso şi i-au adus perfecţionări.

O cheie care se schimbă la fiecare mesaj asigură o rezistenţă mai mare decît una folosită de mai multe ori şi, de aceea, au început să se folosească chei pentru fiecare mesaj nou. Cei

doi au descoperit un mijloc foarte inteligent de a se asigura schimbarea cheii şi anume folosirea chiar a textului clar drept cheie. Procedeul s-a numit sistemul autocheii.

Inventatorul primului procedeu de folosire a autocheii, Cardano, un doctor şi, în acelaşi timp, matematician milanez, a rămas în criptografie mai mult datorită contribuţiei sale la dezvoltarea steganografiei decît datorită noului procedeu. Modul în care a conceput el folosirea noului sistem este defectuos, aşa că nu vom insista asupra lui.

Istoriografia criptologiei a dat dovadă de cea mai crasă eroare şi neglijenţă în legătură cu inventatorul celui de-al doilea procedeu al autocheii. Astfel, a fost ignorată această contribuţie esenţială şi s-a dat numele cunoscutului Blaise de Vigenère unui cifru elementar şi primitiv, cu care el n-a avut nimic de-a face.

Vigenère nu era de origine nobilă, dar la vîrsta de 24 de ani a intrat în slujba ducelui de Nevers, la curtea căruia a slujit toată viaţa, exceptînd unele perioade cînd a fost trimis în străinătate ca diplomat. În 1549, pe cînd avea 29 de ani, a fost trimis la Roma. Aci, Vigenère a luat contact cu problemele criptologiei, care l-au atras în mod deosebit. A citit lucrările lui Trithemius, Belaso, Cardano şi Porta, precum şi manuscrisul lucrării lui Alberti.

În timpul vieţii sale a publicat vreo douăzeci de cărţi pe teme foarte ciudate, dar exceptînd vestitul Traicté des Chiffres, atît de des citat de truditorii din acest domeniu, restul a căzut pradă uitării.

Acest „Traicté" este o lucrare curioasă. În cele peste 600 de pagini sînt cuprinse nu numai cunoştinţele criptologice din vremea aceea, dar şi un amestec ciudat de fapte şi anecdote. Aici se găseşte prima reprezentare europeană a ideogramelor japoneze. În digresiunile sale, Vigenère se ocupă de alchimie, magie, misterele universului, recipiente pentru prelucrarea aurului şi face speculaţii filozofice de tipul „toate lucrurile din lume sînt un cifru".

În ciuda acestor fantasmagorii, Traicté-ul, în ceea ce privește problemele criptologiei, merită toată crezarea. Vigenère a fost foarte scrupulos în ceea ce privește acest domeniu și toate informațiile pe care le dă sînt verificate cu grijă și redate cu acuratețe.

Printre numeroasele cifruri pe care le-a prezentat și comentat, Vigenère s-a oprit îndeosebi asupra cifrurilor polialfabetice. Fiecare din aceste cifruri se baza pe tabloul lui Trithemius, deși Vigenère a așezat alfabete mixte la capul orizontal și cel vertical al tabloului. A înregistrat și comentat o varietate largă de chei: cuvinte, expresii, versuri, data expedierii mesajului, folosirea progresivă a tuturor alfabetelor etc. În cele din urmă, prezintă și procedeul său bazat pe autocheie. La fel ca și Cardano, folosea textul clar drept cheie. Dar, spre deosebire de Cardano, a adus două perfecționări sistemului respectiv. În primul rînd, el a asigurat sistemului o cheie primară, constînd dintr-o singură literă cunoscută atît cifrorului expeditor cît și cifrorului destinatar. Această cheie primară ajuta pe destinatar să poată începe descifrarea. Cu cheia respectivă, el afla prima literă din textul clar, care, la rîndul ei, era cheia celei de a doua litere ș.a.m.d.

În al doilea rînd, Vigenère, spre deosebire de Cardano, nu reîncepe cuvîntul cheie la fiecare cuvînt din textul clar, ci folosește curent, în ordine, toate cuvintele și literele acestui text.

cheie	— DA UNO MD ELETERNE
text clar	— au nom de l'éternel
text cifrat	— XI AHG UP TMLSHIXT

În exemplul de mai sus, litera „D" constituie cheia primară. Procedeul acesta asigură o rezistență destul de mare, fapt care a făcut ca în prezent să fie folosit și la unele tipuri de mașini de cifrat.

Vigenère a mai prezentat și un al doilea procedeu în care, după o cheie primară, autocheia constituie chiar criptograma:

cheie	— DX HEE CO UMXGMABQ
text clar	— au nom de l'éternel
text cifrat	— XH EEC CU MXGANABQO

Acest procedeu are avantajul de a avea o cheie incoerentă, dar, în același timp, lasă cheia la dispoziția criptanalistului.

În ciuda expunerii foarte clare făcută de Vigenère asupra acestor procedee, ambele au fost complet uitate și au intrat în criptologia practică de-abia în secolul al XIX-lea.

Cifrul inspirat din Vigenère folosește azi doar alfabetele standard și o cheie formată dintr-un singur cuvînt care se repetă — un sistem mult mai susceptibil de a fi soluționat decît procedeul autocheii. Tabloul actual al sistemului Vigenère constă dintr-o tabula recta modernă: 26 de alfabete standard, așezate orizontal, fiecare fiind cu o literă mai înainte decît celălalt. Acestea sînt alfabetele cifru. Un alt alfabet normal este așezat pe verticală, în stînga tabloului, acesta fiind alfabetul cheie. Ambii corespondenți trebuie să cunoască cuvîntul cheie. Cifrorul repetă acest cuvînt deasupra literelor textului clar pînă cînd fiecare are un echivalent în cheie, după care caută litera textului clar în alfabetul de deasupra tabloului, iar litera din cuvîntul cheie în alfabetul vertical. Litera aflată la intersecția alfabetului vertical al literei clare cu alfabetul orizontal al literei de cifrat constituie echivalentul folosit pentru cifrare. Pentru a se executa descifrarea, se începe cu litera din cheie, se găsește alfabetul de cifrat, căutînd litera din textul cifrat, după

În ciuda acestor fantasmagorii, Traicté-ul, în ceea ce privește problemele criptologiei, merită toată crezarea. Vigenère a fost foarte scrupulos în ceea ce privește acest domeniu și toate informațiile pe care le dă sînt verificate cu grijă și redate cu acuratețe.

Printre numeroasele cifruri pe care le-a prezentat și comentat, Vigenère s-a oprit îndeosebi asupra cifrurilor polialfabetice. Fiecare din aceste cifruri se baza pe tabloul lui Trithemius, deși Vigenère a așezat alfabete mixte la capul orizontal și cel vertical al tabloului. A înregistrat și comentat o varietate largă de chei : cuvinte, expresii, versuri, data expedierii mesajului, folosirea progresivă a tuturor alfabetelor etc. În cele din urmă, prezintă și procedeul său bazat pe autocheie. La fel ca și Cardano, folosea textul clar drept cheie. Dar, spre deosebire de Cardano, a adus două perfecționări sistemului respectiv. În primul rînd, el a asigurat sistemului o cheie primară, constînd dintr-o singură literă cunoscută atît cifrorului expeditor cît și cifrorului destinatar. Această cheie primară ajuta pe destinatar să poată începe descifrarea. Cu cheia respectivă, el afla prima literă din textul clar, care, la rîndul ei, era cheia celei de a doua litere ș.a.m.d.

În al doilea rînd, Vigenère, spre deosebire de Cardano, nu reîncepe cuvîntul cheie la fiecare cuvînt din textul clar, ci folosește curent, în ordine, toate cuvintele și literele acestui text.

cheie	— DA UNO MD ELETERNE
text clar	— au nom de l'éternel
text cifrat	— XI AHG UP TMLSHIXT

În exemplul de mai sus, litera „D" constituie cheia primară. Procedeul acesta asigură o rezistență destul de mare,

fapt care a făcut ca în prezent să fie folosit și la unele tipuri de mașini de cifrat.

Vigenère a mai prezentat și un al doilea procedeu în care, după o cheie primară, autocheia constituie chiar criptograma :

cheie	— DX HEE CO UMXGMABQ
text clar	— au nom de l'éternel
text cifrat	— XH EEC CU MXGANABQO

Acest procedeu are avantajul de a avea o cheie incoerentă, dar, în același timp, lasă cheia la dispoziția criptanalistului.

În ciuda expunerii foarte clare făcută de Vigenère asupra acestor procedee, ambele au fost complet uitate și au intrat în criptologia practică de-abia în secolul al XIX-lea.

Cifrul inspirat din Vigenère folosește azi doar alfabetele standard și o cheie formată dintr-un singur cuvînt care se repetă — un sistem mult mai susceptibil de a fi soluționat decît procedeul autocheii. Tabloul actual al sistemului Vigenère constă dintr-o tabula recta modernă : 26 de alfabete standard, așezate orizontal, fiecare fiind cu o literă mai înainte decît celălalt. Acestea sînt alfabetele cifru. Un alt alfabet normal este așezat pe verticală, în stînga tabloului, acesta fiind alfabetul cheie. Ambii corespondenți trebuie să cunoască cuvîntul cheie. Cifrorul repetă acest cuvînt deasupra literelor textului clar pînă cînd fiecare are un echivalent în cheie, după care caută litera textului clar în alfabetul de deasupra tabloului, iar litera din cuvîntul cheie în alfabetul vertical. Litera aflată la intersecția alfabetului vertical al literei clare cu alfabetul orizontal al literei de cifrat constituie echivalentul folosit pentru cifrare. Pentru a se executa descifrarea, se începe cu litera din cheie, se găsește alfabetul de cifrat, căutînd litera din textul cifrat, după

care, pe coloana alfabetului de deasupra se află litera din textul clar. De exemplu :

cheie	TYPE TYPE TYPE TYPE TYPE TYPE..
text clar	no is the time for all good...
text cifrat	GMLMLR WIMTMGBI YMGEEJUS...

În mod evident, acest sistem este mai vulnerabil decît originalul Vigenère, deşi o legendă a circulat mult timp, susţinînd că el nu poate fi spart. Faptele aveau să dovedească contrariul.

CONTRIBUŢIA DILETANŢILOR

Telegraful a făcut din criptografie ceea ce este astăzi. În 1845, Francis O. J. Smith a publicat un cod intitulat „Vocabular de corespondenţă secretă adaptat pentru folosirea telegrafului magnetic". În prefaţa acestei lucrări, autorul ei declara că „secretul corespondenţei este de o importanţă deosebită". Această lucrare a stîrnit interesul unui mare număr de intelectuali, oameni de afaceri şi politici pentru scrierile ascunse. Ei şi-au adus din plin contribuţia la îmbogăţirea zestrei de sisteme de cifrare a criptologiei.

Între timp, telegraful — autorul real al revoluţiei criptografice — a dus la apariţia transmisiunilor din armată, iar o dată cu acestea a apărut şi posibilitatea interceptării mesajelor, impunîndu-se cu necesitate o protecţie a lor. Vechile nomenclatoare şi noile coduri nu prezentau garanţii în ce priveşte rezistenţa la criptanaliză şi nu asigurau nici expeditivitatea cerută de mijloacele de comunicare.

Ofiţerii de transmisiuni au părăsit codurile şi nomenclatoarele şi şi-au îndreptat atenţia spre cifruri, care puteau fi tipărite pe o foaie de hîrtie şi distribuite cu uşurinţă tuturor unităţilor interesate. Secretul putea fi asigurat de cheile variabile care se schimbau foarte repede. Cifrurile erau ideale pentru comunicaţiile din zonele fronturilor şi astfel a luat naştere, în perioada respectivă, ceea ce se numeşte cifrul militar.

La dispoziția militarilor se găsea, pe atunci, sistemul Vigenère modernizat. Vechile obiecții împotriva folosirii lui au dispărut o dată cu apariția telegrafului, iar reputația acestuia de a fi indestructibil i-a determinat pe militari să-l adopte fără rezerve.

Apoi, în 1863, un maior de infanterie din armata prusacă a descoperit soluția generală pentru cifrurile bazate pe substituția polialfabetică periodică. Dintr-o singură lovitură, vechea legendă a invincibilității lor s-a spulberat, iar ofițerii de transmisiuni, obligați să asigure secretul mesajelor pe care le transmiteau, au început să caute noi sisteme. Multe idei interesante s-au găsit în scrierile criptologilor diletanți care propuseseră diferite cifruri pentru mesajele particulare.

O mare parte din sistemele acestea de cifrare au devenit clasice și se folosesc cu succes și astăzi.

Unul din sistemele inventate înaintea apariției telegrafului depășea cu mult realizările epocii respective și era atît de mult în spiritul noilor invenții încît se impune să fie tratat împreună cu ele. Acest sistem este în același timp atît de modern în concepție, încît și în ziua de azi, după un secol și jumătate de progres tehnic rapid, continuă să fie folosit. Inventatorul său, Thomas Jefferson, a fost un om politic și de cultură remarcabil. El a inventat „roata de cifrat" pe cînd era secretar de stat și voia să apere secretele S.U.A. față de Anglia și Franța, dar e mai bine să-l lăsăm pe Jefferson să-și explice sistemul de cifrare :

„Luați un cilindru din lemn de vreo cinci centimetri diametru și 15 sau 20 cm lungime. Găuriți-l și introduceți înăuntru un ax. Împărțiți partea exterioară în douăzeci și șase de părți egale (pentru cele 26 litere ale alfabetului) și, cu un vîrf ascuțit, trageți linii paralele prin toate punctele de diviziune de la un capăt la altul al cilindrului. Trageți liniile respective cu cerneală, pentru a fi vizibile, apoi tăiați cilindrul în rotițe, fiecare de aproximativ jumătate de centimetru grosime. Numerotați-le pe părți, în așa fel încît să le puteți aranja în ordinea pe care o doriți. Pe partea exterioară a rotiței, între liniile trase

cu cerneală, treceți toate literele alfabetului, nu în ordinea lor normală, ci la întîmplare, în așa fel încît să nu fie două rotițe la fel. După ce ați terminat această operație, puneți-le pe axul de fier care are la cap o piuliță, pentru a putea strînge și imobiliza rotițele ori de cîte ori doriți. Acum aparatul este gata pentru a fi folosit, dacă, bineînțeles, cei doi corespondenți au fiecare cîte un aparat similar, cu rotițele așezate în mod identic.

Să presupunem că trebuie să cifrăm următoarea propoziție : „Your favor of the 22^{d} is received" :

— întorc prima rotiță pînă apare litera *y;*

— întorc a doua rotiță pînă cînd în dreptul lui *y*, de pe prima rotiță, apare *o;*

— întorc a treia rotiță și-l așez pe *u* de pe aceasta în dreptul lui *o* de pe a doua rotiță ;

— întorc a patra... pînă ce *r* este în dreptul lui *u* de pe a treia...

— întorc a cincea... pînă ce *f* este în dreptul lui *r* de pe a patra;

— întorc și a șasea... pînă ce *a* este în dreptul lui *f* de pe a cincea.

Fac această operație pînă cînd am toate cuvintele din propoziție aranjate într-un singur rînd, apoi strîng rotițele cu șurubul. Veți observa că pe cilindru se găsesc alte 26 de șiruri, nu în serii regulate, ci amestecate, fără să aibă vreun înțeles.

Copiați oricare dintre ele și trimiteți-l corespondentului dumneavoastră. Cînd îl va primi, va aranja rotițele din care-i compus cilindrul, astfel încît să obțină și el șirul pe care i l-ați trimis. După aceasta, fixează rotițele cu ajutorul șurubului, examinează celelalte 25 de șiruri rezultate și găsește unul în care scrie „Your favor of the 22^{d} is received". Pe acesta îl reține, deoarece toate celelalte șiruri nu formează cuvinte inteligibile.

Cînd cilindrul de rotițe este fixat și literele lor amestecate, apare o varietate imensă de cifruri pe care le puteți folosi simultan în corespondența cu diverse persoane care, deși au același aparat, nu vor putea afla secretul mesajelor transmise altcuiva, deoarece sînt criptate cu ajutorul altui cifru".

Un cilindru de 15 cm lungime, divizat în 36 de rotițe, asigură un număr de cifruri care apare ca 372 urmat de 39 de zerouri, fapt ce demonstrează uriașele posibilități de folosire conținute de „roata" lui Jefferson.

Un alt american, colonelul Docius Wadsworth, a inventat un mecanism de cifrat foarte interesant. Inovația lui consta în folosirea alfabetelor de lungimi diferite. Aparatul cu ajutorul căruia a reușit această performanță este format din două discuri de mărimi diferite, confecționate din aramă și introduse într-o casetă rotundă din lemn, cu diametrul de 16 cm și aproape 7,5 cm înălțime. Alfabetul de pe discul mai mare este format din cele 26 litere, plus cifrele de la 2 la 8, ajungîndu-se, astfel, la un total de 33 de elemente. Alfabetul de pe discul mai mic conține 26 de litere. Unul din alfabete este folosit pentru cifrat, iar celălalt reprezintă literele din textul clar. (Wadsworth n-a lăsat nici o indicație prin care să arate care este alfabetul de cifrat și care cel clar). Cele două discuri ale aparatului sînt cuplate între ele prin două roți dințate, una avînd 33 de dinți, iar cealaltă 26. Literele de pe discul mai mare au fost scrise pe niște fișe de aramă care se pot aranja în ordinea dorită de corespondenți. Înainte de a trece la cifrare, cei doi corespondenți trebuie să cadă de acord asupra poziției din care să înceapă rotirea celor două secțiuni. De exemplu : *R* de pe discul mare să fie în dreptul lui *V* de pe discul mic. Pe casetă are un semn, pentru a fi folosit în procesul de cifrare. Să presupunem că avem de cifrat cuvîntul llama, un cuvînt excelent pentru a scoate în evidență modul de funcționare a acestui aparat. Cu ajutorul unui mîner se mișcă discurile pînă cînd *l* ajunge în dreptul semnului de pe casetă. Se scrie litera sau cifra de pe discul mare care a ajuns în același timp în dreptul semnului respectiv. Se învîrte din nou discul pînă cînd *l* apare pentru a doua oară în dreptul semnului respectiv. În timp ce discul mic a făcut o rotație completă, discul mai mare s-a învîrtit doar cu 26/33 dintr-o rotație completă. Drept urmare, a doua literă din textul cifrat se va găsi cu 7 poziții mai înainte în cadrul alfabetului de pe discul mare față de prima literă din același

text. Dacă se repetă cifrarea lui *l* în continuare, prima literă din textul cifrat nu va mai apare pînă la epuizarea celor 33 de elemente de pe discul mai mare, întrucît 26 și 33 nu au factori comuni.

Un alt aparat de cifrat a fost prezentat în 1867 la expoziția universală de la Paris de către savantul englez Wheatstone.

Pe un disc erau scrise în cerc două alfabete, cel exterior format din 27 de semne (26 de litere așezate în ordinea alfabetică, plus un semn folosit ca pauză între cuvinte). În cercul interior se aflau înscrise la întîmplare cele 26 de litere ale alfabetului. Pe disc erau fixate două ace ca cele de ceasornic cuplate cu ajutorul unor rotițe. Wheatstone scria că „în momentul în care începeți cifrarea, acul lung trebuie să fie fixat în dreptul căsuței conținînd semnul folosit drept pauză între cuvinte, iar cel mic să fie așezat în aceeași poziție. Acul mai lung va fi rotit și fixat în dreptul literei din textul clar, iar literele indicate de acul mic formează textul cifrat". Lungimea diferită a celor două alfabete înseamnă că pînă ce acul mare face o rotație completă, acul mic a trecut cu un semn în cea de-a doua rotație.

Deși s-a bucurat de aprecieri, acest aparat este destul de simplu, iar criptograma obținută nu este prea rezistentă la criptanaliză, deoarece diferența doar de o literă dintre cele două alfabete nu permite ca silabele și cuvintele formate din litere care se înșiruie în ordine alfabetică să fie ascunse prea bine și dă criptanalistului posibilitatea să atace criptograma cu multe șanse de succes. De altfel, datorită slabei sale rezistențe, acest sistem a fost soluționat la numai 4 ani după ce fusese expus la Paris.

Un alt englez, Playfair, prieten bun cu Wheatstone, a descoperit un alt sistem de cifru care, grație unei confuzii făcute de către istorici, s-a numit cifrul simetric al lui Wheatstone. Cifrul este literar și digrafic, adică, pentru o singură unitate fonetică din textul clar se folosesc două litere, iar soluția poate fi aflată numai dacă se cunosc ambele elemente. Wheatstone i-a arătat lui Playfair că cifrul descoperit de el poate fi folosit fie sub formă rectangulară, fie sub formă de pătrat, dar curînd

acesta s-a statornicit sub formă de pătrat. Ocupîndu-se în continuare de perfecționarea acestui sistem, Wheatstone a folosit un alfabet de cifrat mixt, pe care l-a obținut prin transpoziție, cu ajutorul unei chei. Procedeul întrebuințat era cu totul nou și constă în următoarele : se scrie cuvîntul cheie și dedesubtul lui restul literelor alfabetului, după modelul de mai jos :

M A G N E T I C
B D F H J K L O
P Q R S U V W X
Y Z

Retranscriind coloanele pe orizontală, a apărut următorul alfabet de cifrat : M B P Y A D Q Z G F R N H S E J U T K V I L W C O X. Ca și în cazul lui Vigenère, această posibilitate de a obține alfabete de cifrat a fost însă pierdută, deoarece s-a recurs la forma cea mai imperfectă pe care o putea îmbrăca procedeul. Cheia a fost transcrisă direct într-un pătrat de 5 x 5, restul elementelor alfabetului înșiruindu-se după modelul expus mai sus. Această formă a slăbit rezistența cifrului, dar a ușurat manevrarea lui. Iată cum arată un astfel de cifru, avînd drept cheie numele propriu PALMERSTON :

P A L M E
R S T O N
B C D F G
H I K Q U
V W X Y Z

Pentru cifrat, textul e împărțit în grupuri de cîte două litere, iar literele duble, cum ar fi *l* din balloon, sînt despărțite între ele printr-un *x*, în așa fel încît cuvîntul respectiv va fi cifrat ca ba/lx/lo/on.

Literele din fiecare pereche pot intra, în funcție de pătrat, în următoarele raporturi : pot apărea pe același rînd, în aceeași coloană sau să nu fie nici pe același rînd, nici pe aceeași coloană. Literele care cad în același rînd sînt înlocuite cu următoarea literă din dreapta. Astfel, *am* = *L E*, *hi* = *I X* și *os* =

N T. Fiecare rînd este considerat ca fiind ciclic, așa că litera care urmează după ultima literă dintr-un rînd este prima din rîndul următor. Astfel, *le* = *MP*, *ui* = *HK*.

Literele care apar în aceeași coloană sînt înlocuite de literele aflate imediat sub ele.

Așadar, *ae* = *SJ*, *of* = *FQ*, *wi* = *AW*, *br* = *HB*. Dacă literele din textul respectiv de cifrat nu apar nici în rîndul nici în coloana pătratului, atunci sînt înlocuite cu literele de pe coloana și rîndul lor. Practic, se procedează astfel : pentru a cifra secvența *sq*, cifrorul trebuie să le caute în pătrat și, o dată identificate, urmărește rîndul literei, pînă cînd acesta întîlnește coloana celei de-a doua litere din secvența respectivă a lui Z.

. . . M .
R S T O N
. . . F .
. . . Q .
. . . Y .

Litera aflată la intersecția șirului care îl conține pe *s* cu coloana în care se află *q* devine prima literă din textul cifrat. Apoi, cifrorul urmărește rîndul celei de-a doua litere, pînă cînd acesta intersectează coloana primei litere.

. A . . .
. S . . .
. C . . .
H IJ K Q U
. W . . .

Litera aflată la intersecția rîndului care îl conține pe *q* cu coloana care îl conține pe *s*, adică *i*, devine cea de-a doua literă din textul cifrat. Descifrarea constă exact în același proces, căci dacă *ow* = *SY*, atunci *sy* = *OW*. În primele două cazuri descrise, literele din textul clar se găsesc la stînga sau deasupra

literelor din textul cifrat. Folosind acelaşi pătrat, un text cifrat se reduce la următoarele :

MT TB BN ES WH TL MP TA LN NL NV
lo rd gr an vi lx le sl et te rz

Z de la urmă este o literă fără valoare, pentru a completa grupa finală.

Avantajul unui astfel de cifru constă, în primul rînd, în aceea că, fiind digrafic, ascunde caracteristicile literelor şi reduce la zero eficienţa metodelor obişnuite de analiză a frecvenţei. De asemenea, înjumătăţeşte numărul de elemente pentru analiza frecvenţei. În al doilea rînd, numărul de digrafe este cu mult mai mare decît numărul literelor simple şi, în consecinţă, caracteristicile lingvistice se împart între mai multe elemente, ceea ce îngreuiază mult individualizarea lor. Există numai 26 de litere faţă de 676 digrafe; cele mai frecvente litere din alfabetul englezesc *e* şi *t* au o frecvenţă medie de 12, şi respectiv 9 la sută; digrafele cele mai frecvente în engleză *th* şi *h* au frecvenţă medie de numai 3,25 şi 2,5 la sută. Cu alte cuvinte, nu numai că sînt mai multe unităţi dintre care trebuie făcută alegerea, dar acestea sînt mult mai puţin diferenţiate între ele.

În Anglia, în 1857, se vindea un carton pe care se afla tipărit cu roşu şi negru un pătrat conţinînd alfabetul. Era un nou sistem de scriere secretă datorat amiralului Francis Beaufort. Plicul în care se găsea acest carton purta următoarele indicaţii :

„Cheia pentru acest tablou poate fi un vers dintr-o poezie ori un nume de persoană sau loc, care nu poate fi uitat uşor... Priviţi la coloana din margine şi căutaţi prima literă din text *(t)*, apoi căutaţi prima literă din cheie *(o)*, după care, urcînd pînă în capul coloanei în care se găseşte litera *v*, veţi găsi litera *c*, care are să fie prima literă din textul cifrat".

Pătratul alfabetic este în esenţă similar cu cel al lui Vigenère, exceptînd doar faptul că el repetă alfabetul normal pe toate cele patru laturi ale pătratului, aşa că pe fiecare margine se găsesc 27 litere şi în fiecare colţ al pătratului se află litera A.

Există şi o altă variantă în care cifrarea începe nu cu litera din textul clar, ci cu cea din cheie. Această variantă s-a numit varianta Beaufort, dar poate fi numită şi varianta Vigenère, deoarece criptanalistul, pentru a o descifra, execută exact operaţiunile de cifrare din sistemul propus de Vigenère : se caută litera din cheie pe margine şi litera din textul cifrat în rîndul prim al pătratului, iar la joncţiunea coloanei acesteia cu rîndul literei din cheie se găseşte litera din textul clar.

Tot în secolul trecut, americanul Pliny Earle Chase, la fel ca şi Beaufort, a acordat pentru o foarte scurtă perioadă de timp atenţie criptografiei, iar rezultatul a fost o invenţie care a deschis noi drumuri în această ştiinţă. Astfel, printre articolele publicate de către Chase în revista *Mathematical Monthly*, se află şi un articol care descrie pentru prima dată un sistem de cifrat fracţional.

La baza acestui sistem se află cercul lui Polybius. Numerele de pe margine şi de pe rîndul de deasupra indică rîndul şi coloana în care se găseşte o anumită literă. Pînă la Chase a apărut o serie întreagă de variante ale acestui careu al lui Polybius, dar nimeni nu şi-a dat seama că simbolurile pot fi manipulate şi că ele nu sînt numai părţi ale întregului. Chase a despărţit cele două coordonate şi le-a supus la diferite tratamente criptografice. El a început cu un careu umplut cu zece coloane de litere greceşti, ca cel pe care-l prezentăm mai jos :

	1	2	3	4	5	6	7	8	9	0
1	x	u	a	c	o	n	z	l	p	φ
2	b	y	f	m	&	e	g	j	q	ω
3	d	k	s	v	h	r	w	t	i	λ

Chase a scris vertical coordonatele, astfel încît cuvîntul clar, Philip, apărea astfel :

1 3 3 1 3 1
9 5 9 8 9 9

Apoi a înmulţit rîndul al doilea cu 9, obţinînd următorul rezultat :

1 3 3 1 3 1
8 6 3 9 0 9 1

Rezultatul a fost retransformat în litere prin resubstituţie cu ajutorul careului, după cum urmează : 8 (singur) = *l*, *j* ori *t*, apoi 16 = *n*, 33 = *s*, 39 = *i* şi aşa mai departe, obţinînd drept rezultat L N S I Ø I X.

Chase a propus şi moduri mai complicate de transformare a rîndului. El a subliniat însă faptul că procedeele simple sînt mai eficace. Sistemele propuse de Chase oferă o rezistenţă mare şi, de asemenea, sînt uşor de manevrat. Cu toate acestea, n-au fost întrebuinţate, deşi erau superioare altora folosite pe timpul acela. Dacă profesorul de matematici din Cambridge, Charles Babbage, a fost primul om care a reuşit să descifreze o criptogramă cu autocheie, precum şi mai multe criptograme care foloseau polialfabetele, cel care a scris prima lucrare unde se arată cum se soluţionează un cifru alfabetic cu chei regulate a fost un ofiţer prusac, maiorul Friedrick W. Kasiski.

Într-o lucrare a sa, „Die Geheimschriften und die Dechiffrir-kunst" a sesizat că repetarea unei părţi din cheie împreună cu repetarea unei părţi din textul clar duc la repetiţie şi în textul cifrat.

Cheie : RUN RUN RUN RUN RUN RUN RUN RUN RUN RUN.

Text clar : to be or not to be that is the question.

Text cifrat : *K I O V* I E E I G *K I O V N U* R N V J *N U* V K H V M G Z I A. De fiecare dată cînd cheia *RUNR* este folosită pentru a cifra *to be*, textul cifrat va fi *KIOV*. Aceleaşi cauze determină acelaşi efect. Identic se petrec lucrurile în cazul lui *UN* din cheie, care operează asupra lui *th* din textul clar, în textul cifrat obţinîndu-se *NU*.

În mod clar, cuvîntul cheie trebuie să se repete o dată sau de mai multe ori într-o anumită parte a textului, pentru a putea cifra în mod identic două grupări de litere aflate la o

oarecare distanţă unele de altele. Numărul de litere dintre cele două repetiţii din textul cifrat arată de cîte ori a fost repetată cheia. Numărătoarea elementelor din acest interval cuprinde o serie de litere care se repetă. Astfel, intervalul dintre primul *KIOV* şi cel de-al doilea cuprinde 9 litere, din care 5 nu se repetă, iar patru se repetă. Acest interval de 9 litere rezultă din faptul că cheia este formată din trei litere şi se repetă de trei ori. Analiza intervalelor dintre repetiţii poate să ne furnizeze lungimea cuvîntului-cheie.

Desigur, nu toate repetiţiile din textul clar duc la repetiţii în textul cifrat. Cei doi *ti* din *that is* şi *question* sînt cifraţi cu digrafe diferite, la fel *st* din *is the* şi *question*. Mai mult decît atît, multe repetiţii din textul cifrat sînt, pur şi simplu, rezultatul unor coincidenţe. De exemplu, *secvenţa th* cifrată cu *CO* va deveni *vv* în sistemul lui Vigenère, dar acelaşi lucru se va întîmpla şi cu *ir* cifrat cu cheia *NE*. Apariţia celor două grupuri *vv* nu reflectă o repetiţie în textul clar. Acest tip de repetiţii sînt denumite repetiţii accidentale, pentru a fi deosebite de adevăratele repetiţii ca *KIOV*.

Repetiţiile accidentale, în mod normal, vor sugera unele date false despre lungimea cuvîntului cheie, însă cele adevărate vor arăta clar care e lungimea acesteia. Ştiind cîte litere sînt în cuvîntul cheie, ştim şi cîte alfabete au fost folosite în cazul cifrului polialfabetic. Aceste informaţii permit criptanalistului să clasifice elementele din criptogramă, în aşa fel încît toate literele cifrate cu ajutorul primei litere din cheie să formeze un grup, cele cifrate cu ajutorul celei de-a doua litere din cheie, un alt grup şi aşa mai departe. Deoarece toate, să zicem, *e*-urile din primul grup au fost substituite cu ajutorul unei singure litere din cheie în aceeaşi literă din textul cifrat, toate *a*-urile într-o singură literă de text cifrat şi aşa mai departe, fiecare din aceste grupe de litere constituie un cifru de substituţie monoalfabetică şi, în felul acesta, poate fi soluţionat.

Un exemplu ne va ajuta să facem foarte clare cele spuse mai sus. Luăm următoarea criptogramă :

ANYVG YSTYN RPLWH RDTKX
RNYPV QTGHP HZKFE YUMUS AYWVK ZYEZM
EZUDL JKTUL JLKQB JUQVUECKBN RKTHP
KESXM AZOEN SXGOL PGNLE EBMMT GCSSV
MRSEZ MXHLA KJEJH TUPZU EDWKN NNRWA
GEEXS LKZUD LJKFI XHTKP IAZMX FACWC
TQIDU WBRRL TTKVN AJWVB REAWT NSEZM
OECSS VMRSL JMLEE BMMTG AYVIY GHPEM
YFARW AOAEL UPIUA YYMGE EMJQK SFCGU
GYBPJ BPZYPJASNN FSTUS STYVG YS

Repetițiile de cîte trei litere sau mai multe au fost evidențiate. Cele digrafice au fost ignorate, deoarece sînt prea frecvente, deși în criptogramele mai scurte sînt de un real folos. Frecvența fiecărei litere este următoarea :

E	S	M	Y	T	A	K	U	L	N	P	G	J	R	Z	V	W	B	H	C
22	18	16	16	15	14	14	14	13	13	13	12	11	11	11	10	9	8	8	7

X	F	D	I	Q	O
7	6	5	5	5	4

Acest rezultat diferă foarte mult față de cel obținut în cazul substituțiilor monoalfabetice. Toate cele 26 de litere pot apărea de cîteva ori sau, în cazul unei criptograme mai lungi, unele pot lipsi. Nici una din litere nu iese în relief în mod deosebit. Cele mai frecvente se întîlnesc doar în proporție de 7,7% și 6,3%.

Nu apar nici grupe de litere de frecvență înaltă, medie, joasă sau mică. Avem de-a face cu o descreștere lină, rezultat al dispersării literelor individuale în cîteva alfabete.

O dată localizate repetițiile, Kasiski a sugerat să se calculeze distanțele care le separă unele de altele și, apoi, să fie aflați factorii cu care sînt divizibile. Factorul întîlnit cel mai des indică numărul de litere care formează cuvîntul-cheie. Criptanaliștii fac deseori această operație — numită în prezent și „examinarea Kasiski" — sub formă de tabel.

Repetiția	Poziția		Interval	Factorii
repetiția	prima	a doua	intervalul	factorii
YVGYS	3	283	280	2 x 2 x 2 x 5 x 7
STY	7	281	274	2 x 137
GHP	28	226	198	2 x 3 x 3 x 11
ZUDLJK	52	148	96	2 x 2 x 2 x 2 x 2 x 3
LEEBMMTG	99	213	114	2 x 2 x 19
SEZN	113	197	84	2 x 2 x 3 x 7
ZMX	115	163	48	2 x 2 x 2 x 2 x 3
GEE	141	249	108	2 x 2 x 3 x 3 x 3

Cel mai frecvent factor este *2*, care apare în fiecare caz, dar deoarece *2* este factor în orice număr cu soț și deoarece foarte rar se folosesc chei din două sau trei litere, criptanaliștii iau în considerație numai numerele de la *4* în sus. În tabelul prezentat, *4* sau *2* x *2* este întîlnit în cinci din cele opt intervale, *5* într-un singur interval, *6* în șase intervale, *7* în două, *8* în două, *9* în două, *12* în patru și celelalte (exceptînd multiplii acestor numere) doar o singură dată.

La început, *6* pare să fie cea mai bună alegere luîndu-se criteriul frecvenței.

Criptanalistul retranscrie criptograma în rînduri de cîte șase litere, punînd una sub alta toate literele despre care se crede că au fost cifrate cu același alfabet. Apoi ia separat fiecare coloană și încearcă să afle echivalentele din textul clar pentru fiecare dintre ele. În cazul criptogramei noastre, în prima coloană se găsesc 48 de litere, fiecare fiind cifrată cu ajutorul primei litere din cuvîntul-cheie (dacă *6* este adevăratul număr de litere din cheie) și acestea sînt prima, a șaptea, a treisprezecea etc., literă din criptogramă, după cum urmează:

A S L K V H U W Z L J U K H M S G M S Z K U W W S L H Z W U T J A Z S J M V E W U Y J G J J S Y.

Deşi contează prea puţin, totuşi frecvenţa literelor în această coloană reflectă o substituţie monoalfabetică şi nu o frecvenţă polialfabetică.

In cazul de faţă, situaţia frecvenţei literelor se prezintă astfel :

2	0	0	0	1	0	2	4	0	5	3	3	3	0	0	0	0	5	1	4	2	4	0	2	4
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	T	U	V	W	X	Y	Z

Rezultatul este încurajator, chiar şi numai pentru faptul că prima prezumţie, conform căreia 6 ar fi numărul de litere din cuvîntul cheie, este corectă.

Pentru ochiul experimentat, frecvenţa literelor în cazul nostru scoate în relief un profil normal al frecvenţei în alfabetul englezesc.

Dacă atît alfabetul clar (alfabetul englezesc în cazul nostru) cît şi cel folosit pentru cifrat sînt cunoscute, ambele fiind alfabete normale, identificarea unei singure litere ajută la identificarea instantanee a tuturor celorlalte. De multe ori ne ajută în această operaţiune literele de joasă frecvenţă. Frecvenţa obţinută în cazul de faţă ne arată că porţiunea cu cea mai joasă frecvenţă este N O P Q R, ceea ce, în alfabetul normal, coincide cu V W X Y Z. Folosindu-ne de aceste date, încercăm să obţinem echivalentul literelor cifrate, după modelul de mai jos :

Clar : i j k l m n o p q r s t u v *w x y z* a b c d e
Cifrat : A B C D E F G H I J K L M *N O P Q* R S T U V W
Clar : f g h
Cifrat : X Y Z

Din tabel rezultă că *i* este substitutul lui *A*, *j* al lui *B*, *k* al lui *C* etc.

Această înşiruire poate fi ciclată astfel încît litera clară *a* să apară la început, avînd însă grijă ca echivalenţii literă clară = literă cifrată să rămînă aceeaşi.

Aceşti echivalenţi, pentru cele 48 de litere din textul cifrat cu prima literă din cuvîntul cheie, sînt următorii :

Cifrat : A S L K V H U W Z L J U K H M S G M S Z K U W
Clar : i a t s d p c e h t r c s p u a o u a h s c e

Cifrat : W S L H Z W U T J A Z S J M V E W U Y J G J J S Y
Clar : e a t p h e c b r i h a r u d m e c g r o r r a g

O astfel de grupare este acceptabilă şi pare să ne ofere soluţia.

Totuşi, lucrul cel mai important pe care l-a aflat criptanalistul, după apariţia profilului normal al alfabetului, este faptul că are de-a face cu un cifru de tip Vigenère. Această descoperire dă posibilitatea folosirii mai multor tehnici, bazate mai ales pe faptul că alfabetul este cunoscut. Metodele întrebuinţate aici sînt valabile şi pentru alte alfabete, dacă acestea sînt cunoscute criptanalistului şi dau rezultate deosebite în cazul alfabetelor de tip Vigenère.

Una din aceste metode, care identifică literele în mod mecanic, foloseşte nişte fişii de carton pe care alfabetul e tipărit de două ori. Literele de înaltă frecvenţă se tipăresc în diferite nuanţe de roşu, iar celelalte în negru. Criptanalistul aşază aceste fişii una sub alta pentru a putea aranja în aceeaşi formaţie literele din coloanele textului cifrat. Apoi trece la căutarea coloanei care conţine litere cu cea mai mare frecvenţă în textul respectiv.

Teoria probabilităţilor permite să se presupună că o coloană conţinînd litere de un roşu foarte închis este corectă în proporţie de 42 la sută, dacă are 9 asemenea litere; în proporţie de 61%, dacă are 12 litere şi în proporţie de 74%, dacă are 15 litere.

Dacă se ia şi următoarea coloană, atunci probabilitatea creşte la 74%, 85% şi 90%. Un neajuns al acestei metode este acela că 9 litere — cele mai des întîlnite — reprezintă o treime din alfabet, ceea ce înseamnă că majoritatea coloanelor vor fi colorate în roşu. Totuşi, se poate evita acest neajuns, eliminîndu-se coloanele care conţin litere rare şi pe care le vom scrie cu albastru. În tabelul de mai jos aceste litere vor fi eviden-

țiate. Ele sînt în număr de cinci (*j, k, q, x, z*) și împreună au o frecvență de aproximativ 2%.

Criptanalistul nu va greși dacă va trece peste coloanele care conțin trei sau mai multe din literele evidențiate.

Cifru	textul clar posibil
N	n o p *q* r s t u v w *x* y *z* a b c d e f g h i *j* *k* l m
T	t u v w *x* y *z* a b c d e f g h i *j* *k* l m n o p *q* r s
W	w *x* y *z* a b c d e f g h i *j* *k* l m n o p *q* r s t u v
X	*x* y *z* a b c d e f g h i *j* *k* l m n o p *q* r s t u v w
Q	*q* r s t u v w *x* y *z* a b c d e f g h i *j* *k* l m n o p
Z	*z* a b c d e f g h i *j* *k* l m n o p *q* r s t u v w *x* y
M	m n o p *q* r s t u v w *x* y *z* a b c d e f g h i *j* *k* l
V	v w *x* y *z* a b c d e f g h i *j* *k* l m n o p *q* r s t u
M	m n o p *q* r s t u v w *x* y *z* a b c d e f g h i *j* *k* l
J	*j* *k* l m n o p *q* r s t u v w *x* y *z* a b c d e f g h i

Prin urmare, numai coloana care începe cu literele *f, l, o, p*, este acceptabilă. Punînd aceste litere alături de cele care le preced în textul clar, ne vom convinge imediat că am făcut o alegere bună.

1 2 3 4 5 6

A N Y V G Y
i f
S T Y N R P
a l
L W H R D T
t o
K X R N Y P
s p
V Q T G H P
d i
U M U S A Y
c e
W V K Z Y E
e n
Z M E Z U D
h e

L J K T U L
t b
J L K Q B J
r d
U Q V U E C
c i
K B N R C T
s t
H B K E S X
p h

Criptanalistul continuă în acest fel, atît cît crede necesar, încercînd să deducă ori să ghicească unele litere sau cuvinte.

De exemplu, el știe că pentru a forma articolul hotărît din limba engleză *the*, *h* cere să fie precedat de *t*. În sistemul Vigenère, alfabetul literei cheie *K* este acela care ne dă rezultatul *T* = *e*. Se verifică rezultatul și se constată că este corect. Tot corecte se dovedesc și coloanele *e, l, n, t, a, v, m*.

În cele din urmă se descoperă că cheia după care s-a făcut cifrarea este cuvîntul SIGNAL, iar textul clar următorul : „If signals are to be displayed in the presence of an enemy, they must be guarded by ciphers. The ciphers must be capable of frequent changes. The rules by which these changes are made must be simple. Ciphers are undiscoverable in proportion as their changes are frequent and as the messages in each change are brief“ [1].

Cea mai bună repetiție din criptograma analizată LEEBMMTG a rezultat din cifrarea întîmplătoare a cuvîntului frequent cu cheia GNALSIGN, iar următoarea repetiție ZUDIJK din cifrarea lui must be 's cu cheia NALSIG. Pe de altă parte, repetarea de trei ori a cuvîntului ciphers și de patru ori a lui change n-a apărut în textul cifrat, deoarece fiecare a fost cifrat cu alte litere din cuvîntul cheie. Repetiția, cu totul întîmplătoare, a lui YVGYS a rezultat din folosirea cheii GNALS pentru cifrarea lui signa și apoi a cheii SIGNA pentru literele gnals. Repetiții accidentale, de mai mult de trei litere, sînt extrem de rare, dar se pot întîlni.

Ce se întîmplă dacă alfabetele folosite sînt necunoscute ? Criptanalistul e nevoit să le afle literă cu literă. Cea mai mică descoperire poate duce la identificarea întregului alfabet. De obicei, se recurge la diverse analize lingvistice pe baza contactelor, a frecvenței etc. și se fac o serie de prezumții, toate conform cu regulile folosite în cazul substituției monoalfabetice.

[1] În limba română : „Dacă semnalele urmează să fie emise în pre-
zența unui inamic, acestea trebuie apărate cu ajutorul cifrurilor. Cifru-
rile trebuie să dea posibilitatea unor schimbări frecvente. Regulile după
care aceste schimbări urmează să se efectueze trebuie să fie simple.
Rezistența la descifrare este cu atît mai mare, cu cît cifrurile se schimbă
mai des, iar mesajele cifrate cu ajutorul lor sînt mai scurte“.

Se substituie prezumțiile în criptogramă și se construiește textul clar bucățică cu bucățică, deseori descoperindu-se cheia și alfabetele de cifrat. Pentru a avea șanse de succes în folosirea acestei metode, sînt necesare criptograme lungi, ca să fie cîte 40—60 de elemente pentru fiecare literă din cuvîntul cheie.

PROFESORUL, SOLDATUL ȘI OMUL DE GENIU

Profesorul de germană Auguste Kerckhoffs a intrat în istoria criptologiei mai ales datorită lucrării sale „La Cryptographie militaire", aceasta fiind cea mai concisă carte de criptologie din cîte s-au scris vreodată. În 64 de pagini, autorul a cuprins toate cunoștințele din domeniul criptologiei, inclusiv polialfabetele și alfabetele mixte existente pe vremea lui.

Însă ceea ce face din cartea lui Kerckhoffs o lucrare capitală este faptul că autorul încearcă să răspundă problemelor puse criptologiei de noile condiții, iar soluțiile propuse de el sînt valabile, bine fundamentate și meritorii. Principala problemă constă în a găsi un sistem de criptare care să corespundă cerințelor noului sistem de comunicații creat prin apariția telegrafului. Kerckhoffs și-a propus să afle care sînt principiile după care să fie evaluat orice cifru ce urmează a fi folosit pe timp de război.

În acest sens, el a făcut o diferență între sistemele de comunicare militare de dinainte și de după apariția telegrafului și a arătat că un sistem de criptografie militară trebuie să îndeplinească o serie de cerințe ca : simplitate, rezistență, expeditivitate etc. Această subliniere a noilor cerințe constituie prima contribuție a lui Kerckhoffs la dezvoltarea criptologiei.

A doua constă în reafirmarea principiului conform căruia numai criptanalistul poate afla care este rezistența unui sistem de cifrare.

Reacționînd împotriva modului simplist în care se analiza un sistem de cifrare, precum și împotriva încrederii nejustificate în aceste sisteme, Kerckhoffs a demonstrat că criptanaliza este singura modalitate de dezvoltare a criptologiei și de aflare a adevărului despre diferite sisteme de criptare.

Din aceste două principii fundamentale în alegerea de cifruri pentru armată, Kerckhoffs a dedus șase cerințe specifice : 1) sistemul trebuie să fie indestructibil, dacă nu în teorie cel puțin în practică; 2) sistemul trebuie să fie ușor de înțeles și să nu constituie un inconvenient pentru corespondenți; 3) cheia să fie ușor memorabilă și ușor de schimbat; 4) criptogramele să fie transmisibile cu ajutorul telegrafului; 5) aparatul sau documentele necesare criptării și decriptării să fie portabile și să poată fi memorate de o singură persoană; 6) sistemul trebuie să fie ușor, să nu ceară cunoașterea unei liste de reguli și să nu implice consumarea unei energii intelectuale prea mari.

Aceste cerințe cuprind idealul la care țintiseră toate sistemele de cifru militare. Niciodată, pînă în prezent, nu s-a reușit ca toate aceste cerințe să fie satisfăcute de unul și același cifru. Cel mai adesea, prima cerință este sacrificată. Kerckhoffs a militat mult timp împotriva părerii că un cifru militar trebuie să reziste soluționării pînă cînd ordinele care au fost transmise cu ajutorul lui au fost executate. El a subliniat faptul că „unele comunicări la mari distanțe își păstrează caracterul secret o perioadă mai mare de timp". Avea dreptate, dar un astfel de cifru n-a fost încă inventat și, de aceea, criptografia militară se bazează și în prezent pe cifruri care întîrzie soluționarea criptogramei și nu pe cifruri indestructibile.

Cea de-a doua cerință pare foarte curioasă la prima vedere. Kerckhoffs a explicat că, prin „sistem", el înțelege „partea materială a procesului de cifrat : tablouri, coduri și orice tip de aparat mecanic necesar pentru criptare" și nu „cheia propriu-zisă". Kerckhoffs face, astfel, pentru prima oară distincție, astăzi capitală în criptografie, între sistemul general și cheia specifică. De ce trebuie ca un sistem general să nu fie secret și de ce un anumit cifru trebuie să fie secret ? „Deoarece,

a răspuns Kerckhoffs, nu-i greu să înțelegem că un sistem care necesită multă pază, fiind în mîna mai multor indivizi, poate fi compromis oricînd". Practica a dovedit că acesta este adevărul. Cea de-a doua cerință formulată de Kerckhoffs a fost larg acceptată și reformulată astfel : „Inamicul, deși cunoaște sistemul general de criptare, nu trebuie, totuși, să poată soluționa mesajele criptate cu ajutorul lui fără a cunoaște cheia". Cu alte cuvinte, secretul, după Kerckhoffs, trebuie să rezide numai în cheie.

Dacă Kerckhoffs ar fi publicat numai aceste lucruri și-ar fi asigurat un loc în panteonul criptologiei, dar el a făcut mai mult. A pus la punct două metode de criptanaliză care joacă roluri de importanță capitală în majoritatea soluționărilor moderne.

Prima este suprapunerea și constituie cea mai generală soluție pentru sistemele bazate pe substituție polialfabetică. Cu cîteva excepții, această metodă nu impune nici un fel de restricții asupra lungimii cheii, așa cum presupune metoda Kasiski, nici asupra numărului de alfabete care pot avea legătură unele cu altele sau pot fi independente. Ceea ce reclamă o asemenea metodă sînt cîteva mesaje în aceeași cheie. Criptanalistul orînduiește aceste mesaje unul sub altul, astfel încît toate literele cifrate cu aceeași literă formează o singură coloană. Kerckhoffs a demonstrat acest procedeu cu 13 mesaje scurte, cifrate cu ajutorul unei chei lungi. El a procedat astfel :

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	. . .
Mesajul 1	U	H	Y	B	R	J	I	M	B	C	F	A	M	M	T	. . .
Mesajul 2	U	H	W	P	R	B	Q	L	K	I	B	L	W	R	E	. . .
Mesajul 3	I	E	W	H	C	H	Q	K	Q	M	T	M	V	G	J	. . .
Mesajul 4	U	W	V	R	R	H	I	K	M	C	W	W	E	G	H	. . .
Mesajul 5	U	H	S	H	A	M	K	S	V	C	J	W	Z	V	X	. . .

Întrucît a fost folosită o singură cheie pentru cifrarea tuturor mesajelor, este clar că prima literă din cheie a ajutat la criptarea primei litere din fiecare mesaj. Deci, pe coloană apare unul din alfabetele de cifrat care nu constituie altceva

decît o substituție monoalfabetică obișnuită, atacabilă după metoda frecvenței literelor. Același lucru este adevărat și cu privire la celelalte coloane. Însă nu întotdeauna se poate proceda în acest mod, ci numai în cazurile în care în fiecare mesaj cheia se reia de la capăt. De exemplu, avem cuvîntul cheie „PATRIE" și mai multe mesaje. În fiecare mesaj, prima literă va fi cifrată cu ajutorul lui *P*, indiferent dacă cifrarea mesajului precedent s-a încheiat sau nu cu alfabetul de cifrat generat de litera *e*. Există cazuri în care cifrarea mesajului următor nu începe cu *P*, ci, de exemplu, cu *T*, deoarece în mesajul anterior ultima literă din cheie folosită pentru cifrare a fost *A*. Cu alte cuvinte, se poate spune că este vorba de cifrarea unui singur mesaj foarte lung, dar care s-a făcut pe bucăți. În cazul acesta, criptanalistul trebuie să găsească cîteva repetiții pentru a putea face o suprapunere adecvată.

Metoda suprapunerii nu cere ca alfabetul din prima coloană să aibă vreo legătură cu cel din a doua. Ea însă depinde de mărimea coloanei. Kerckhoffs și-a dat seama de acest lucru și a arătat că în cazul în care cheia a fost scurtă și se poate stabili că două coloane sînt cifrate cu aceeași literă, atunci posibilitatea obținerii succesului se dublează. Acest fapt este de mare valoare la cheile periodice, ale căror alfabete de cifrat sînt folosite în mod neregulat în funcție de frecvența literelor din cheie. Dacă toate coloanele cifrate cu ajutorul cheii *e* pot fi recunoscute, adunate și soluționate, aproximativ 12% din text (cazul limbii engleze) va fi soluționat. Coloanele cifrate în mod identic pot fi recunoscute găsind coloanele care au aceeași frecvență de litere.

Kerckhoffs a mai descoperit și un alt mod de a descifra o criptogramă. Spre deosebire de majoritatea metodelor de criptanaliză care caută textul clar, această metodă studiază literele textului cifrat — care sînt convertite apoi în text clar. Această metodă poate fi considerată ca una din cele mai puternice arme din arsenalul criptanalistului. Kerckhoffs a numit-o „simetria de poziție".

Cum acționează, se poate observa privind un tablou cu alfabete mixte :

clar	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p
cifrat —	N	E	W	Y	O	R	K	C	I	T	A	B	D	F	G	H
—	E	W	Y	O	R	K	C	I	T	A	B	D	F	G	H	J
—	W	Y	O	R	K	C	I	T	A	B	D	F	G	H	J	L
—	Y	O	R	K	C	I	T	A	B	D	F	G	G	J	L	M
—	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.

clar	q	r	s	t	u	v	w	x	y	z
cifrat —	J	L	M	P	Q	S	U	V	X	Z
—	L	M	P	Q	S	U	V	X	Z	N
—	M	P	Q	S	U	V	X	Z	N	E
—	P	Q	S	U	V	X	Z	N	E	W
—	.	.	.	.	.	.	.	.	.	.

Este evident că *N* și *E* sînt una lîngă alta în fiecare alfabet de cifrat din acest tablou (considerînd alfabetele ca fiind ciclice). De asemenea, *N* este separat de *Y* printr-un interval format din trei litere, *R* se află cu șase litere înaintea lui *B* etc. Astfel de relații pot fi stabilite între diferite litere din alfabetele respective, așa că, în cazul în care criptanalistul stabilește distanța dintre două litere din textul cifrat într-un alfabet și găsește una din aceste litere în alt alfabet, el poate plasa cea de-a doua literă la distanța cunoscută. Aceasta înseamnă că se stabilește un echivalent cifrat pe care nu l-a avut înainte și care poate fi înlocuit în toată criptograma pentru a adăuga cîteva date care să ajute unei soluționări rapide.

De exemplu, să presupunem că criptanalistul a stabilit, rezolvînd un mesaj pe baza tabloului Vigenère, că *K* și *H* reprezintă literele clare *e* și *n*. În consecință, în alfabetul cifrat, *K* și *H* se găsesc la un interval de nouă litere una de alta :

clar	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p...
alfabet de cifrat					K									H		
distanța					0	1	2	3	4	5	6	7	8	9		

Apoi, să presupunem că, în alt alfabet, el a descoperit că litera de cifrat *K* îl reprezintă pe *i* din textul clar. Se numără 9 spaţii după *K*, astfel :

clar	a b c d e f g h i j k l m n o p q r s t u ...
alfabetul de cifrat nr. 2	K
distanţa	0 1 2 3 4 5 6 7 8 9

şi se operează în întreg alfabetul identitatea $H = r$. Dacă se află, de exemplu, că litera *e* din textul clar este cifrată, în acest alfabet cu *W*, el va măsura distanţa dintre *K* şi *W* (patru litere înainte) şi îl va pune pe *W* cu patru spaţii înaintea lui *K* în primul alfabet de cifrat, găsind litera *b* din textul clar. Deoarece intervalele dintre litere rămîn fixe pentru toate alfabetele de cifrat din acest tablou, identificarea corectă a cîtorva litere din alfabete diferite duce la stabilirea celorlalte.

Kerckhoffs s-a oprit aici. Criptanaliştii au observat acelaşi lucru cînd au construit scheletul tablourilor pentru substituţii polialfabetice şi cînd rezolvau, mai ales, sisteme bazate pe alfabetul *a-z*. Criptologii moderni au descoperit, de asemenea, că principiul distanţelor liniare include atît proporţii orizontale cît şi verticale. Uneori, asemenea înlocuiri în lanţ duc la reconstituirea tabloului întreg. Cel mai adesea însă, îi asigură criptanalistului noi echivalente sau îi notifică că o anumită prezumţie contrazice regula şi, deci, este nejustă. Simetria latentă a poziţiilor este o metodă indispensabilă pentru un criptanalist modern.

Kerckhoffs şi-a încununat opera prin popularizarea alunecătorului criptografic, demonstrîndu-i identitatea cu tabloul polialfabetic. El a numit alunecător criptografic „Sistemul St.-Cyr", după academia militară franceză unde se preda acesta. Un astfel de aparat constă dintr-o bucată lungă de hîrtie sau carton, numită stator, un alfabet în care literele sînt tipărite la distanţe egale una de alta şi două găuri tăiate la marginile alfabetului. Prin acestea era trasă o fişie lungă de hîrtie (alunecătorul) pe care alfabetul era tipărit de două ori.

Alfabetul de pe stator reprezintă alfabetul textului clar, iar alfabetul de pe alunecător alfabetul de cifrat.

Dacă ambele alfabete sînt în ordinea normală, acest aparat dă naştere unei versiuni prescurtate a tabloului lui Vigenère, deoarece orice alfabet din tabloul respectiv poate fi reprodus, găsindu-i-se cheia pe alfabetul alunecător şi aşezînd-o sub literă *A* a alfabetului de pe stator.

Cu ajutorul acestui dispozitiv, dacă literele nu sînt aşezate în ordinea normală, se obţin alfabete mixte. Kerckhoffs a subliniat că rezultatul obţinut cu acest dispozitiv poate fi obţinut şi cu ajutorul unui disc. Astfel, el a pus alături tabloul, discul de cifrat şi „Sistemul St.-Cyr", arătînd că toate fac parte din aceeaşi familie, diferind unul de altul numai prin formă.

Aceasta este contribuţia lui Kerckhoffs la dezvoltarea criptologiei şi acestea sînt faptele care fac din „Criptographie militaire" o carte remarcabilă.

Cartea lui Kerckhoffs a situat Franţa în fruntea ţărilor cu cea mai dezvoltată criptografie şi, totodată, a dat un imbold neaşteptat activităţilor din acest domeniu. O serie de amatori şi profesionişti au căutat şi descoperit noi sisteme de cifrare, dar majoritatea lor erau lipsite de originalitate, mulţi dintre ei condensînd şi mai mult opera lui Kerckhoffs.

Un ofiţer de infanterie şi asistent al unui prefect de poliţie, marchizul Gaëtan de Viaris, a început să se intereseze de criptografie şi a inventat unele dintre primele maşini de cifrat care asigură şi tipărirea, după cifrare, a criptogramei. Mecanismul maşinii era foarte simplu, singura operaţie pe care trebuia să o facă criptograful fiind aceea de a apăsa pe un buton care imprima litera de cifrat pe o fişie de hîrtie. De asemenea, el a publicat pentru prima oară ceea ce s-au numit „ecuaţii criptografice".

În articolele apărute în publicaţia ştiinţifică Le Gènie Civil, numerele din 12 şi 19 mai, de Viaris propunea ca litera greacă χ (chi) să înlocuiască orice literă din textul cifrat, gamma (γ) orice literă din cheie şi *c* orice literă din textul clar. Apoi, el a demonstrat că formula $c + \gamma = \chi$ dă o cifrare de tipul Vigenère, aceeaşi ca şi cea obţinută prin manipularea standard a tabloului, alunecătorului sau discului. Dacă literele

alfabetului sînt numerotate de la 0 la 25, după modelul de mai jos:

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

tabloul Vigenère poate fi duplicat matematic, adunîndu-se valorile pentru litera clară și cea din cheie și apoi transformînd suma (mai mică de 26) într-o literă corespunzătoare. De exemplu, o cifrare după tabloul standard a literei clare *d* cu ajutorul cheii *G* dă litera cifrată *j*. Cu ajutorul formulei, aceleași litere dau $3+6=9$ sau litera *j*. Un alt cifru va avea, desigur, o altă formulă. Pentru cele trei mari sisteme polialfabetice moderne cu alfabete normale, formulele sînt (folosind notația modernă $P=$ litera clară, $K=$ litera din cheie, $C=$ litera cifru):

	Cifrat	*Descifrat*
Vigenère	$P+K=C$	$C-K=P$
Varianta Vigenère	$P-K=C$	$C+K=P$
Beaufort	$K-P=C$	$K-C=P$

Simetria acestor formule arată clar, aproape grafic, că Beaufort este o substituție reciprocă și că Varianta Vigenère și Vigenère sînt operațiuni inverse. Aceasta este o demonstrație clară a modului în care matematica luminează arhitectura cifrurilor, reliefîndu-i contururile dintr-o singură străfulgerare.

Matematica aplicată criptologiei a fost cea mai inteligentă idee a lui Viaris, dar nu i s-a dat prea mare atenție în 1880.

Paul Valério, un căpitan de artilerie, a publicat în 1892 o lucrare, „De la cryptographie", foarte detaliată, dînd sisteme de cifruri, soluții și coduri. Lucrarea a avut un caracter exhaustiv, adăugînd totuși foarte puțin la ceea ce era deja cunoscut în criptografie, dar înțelegerea criptografiei de către autor a fost așa de completă încît a dat un sentiment de certitudine, siguranță și soliditate acestei științe, sentiment care lipsea criptologilor.

Étienne Bazeries este cel mai mare pragmatist al criptologiei. Contribuția lui teoretică este neglijabilă, dar el este unul din cei mai mari criptanaliști înnăscuți din cîți a cunoscut istoria. Criptograme istorice, invenții noi, sisteme oficiale, mesaje clandestine ale complotiștilor, toate se spărgeau ca nucile sub lovitura ciocanului, cînd ajungeau în mîna lui Bazeries. A fost ofițer, dar, o dată cu cîștigarea reputației de criptanalist, a lucrat la Ministerul de Externe și în poliție.

Disprețul lui față de cifrurile oficiale l-au determinat să alcătuiască două sisteme personale, dar ambele au fost respinse, pe motiv că erau foarte complicate. Un ofițer i-a sugerat ideea că ar avea mai mult succes dacă ar inventa un aparat pe care l-ar putea folosi orice funcționar fără a fi nevoit „să-și stoarcă prea mult creierii".

Bazeries a reluat unul din sistemele sale, care folosea 20 de alfabete diferite, și a inventat „criptograful cilindric". În mod practic, acest criptograf era identic cu roata de cifrat a lui Jefferson, exceptînd doar faptul că avea numai 20 de discuri cu 25 de litere pe circumferințele lor, în loc de 36 de discuri, și care conțineau întreg alfabetul.

Nici acest aparat n-a fost adoptat de Ministerul de Război, iar marchizul de Viaris s-a ambiționat să soluționeze trei mesaje trimise lui de către Bazeries și astfel a dat un suport deciziei luate de armată.

Metoda de soluționare cere ca criptanalistul să fie în posesia aparatului. Această presupunere era în concordanță cu principiul lui Kerckhoffs, conform căruia nici un sistem de cifrare militar nu trebuie să presupună ca aparatul folosit în cifrare să fie secret.

Bazeries a acceptat principiul și a ținut secretă doar cheia — ordinea în care discurile erau plasate pe ax — fiind sigur de imposibilitatea rezolvării mesajului. În metoda folosită de Viaris și care astăzi îi poartă numele, criptanalistul începe

prin a întoarce discurile în aşa fel încît numai litera *a* se află pe rîndul „clar". Fiecare rînd succesiv — numit generatrix — cuprinde toate echivalentele textului cifrat care pot exista pentru *a* pe respectivul generatrix. Mai mult decît atît, aranjamentul echivalenţilor pe fiecare generatrix diferă de celelalte. De exemplu, primii doi generatrix sub *a* în aparatul lui Bazeries erau :

nr. discului	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
text clar	a	a	a	a	a	a	a	a	a	a	a	a	a	a	a	a	a	a	a	a
generatrix 1	B	E	E	Z	Z	Z	L	V	R	F	N	I	U	T	J	I	B	B	C	C
generatrix 2	C	I	B	Y	X	X	O	D	Y	N	D	C	X	I	B	M	C	C	H	F

Pentru a construi alfabete uşor de reţinut, Bazeries folosea chei de tipul : „Doamne apără Franţa", „Onoare şi patrie" sau „Feriţi-vă de curent", „Instruiţi tineretul" ori expresii ca : „Îmi place ceapa prăjită în ulei". Alte alfabete ar produce alte modele.

Aceşti doi generatrix folosesc diferite litere pentru a-l substitui pe *a*.

Criptanalistul poate să prezume că un cuvînt sau o parte din cuvînt, cum ar fi *ation* din criptogramă, a fost cifrat în întregime pe unul din generatrixurile aflate înaintea lui. Atunci el ia toate substitutele posibile pentru *a*, *t*, *i*, *o* şi *n* şi le aşază în coloane una lîngă alta. Aceste coloane le suprapune pe criptogramă, căutînd un grup de cinci litere în care prima literă apare printre substitutele lui *a*, a doua printre substitutele lui *t* şi aşa mai departe. Orice grup de acest fel, în mod evident, poate constitui un posibil echivalent pentru *ation*.

Să presupunem că criptanalistul a găsit un asemenea grup. Dacă substitutul pentru *a* în acel grup este *v*, discul folosit trebuie să fi fost numărul *8*. Este singurul disc care substituie *a*

cu *v* pe primul generatrix. Dacă substitutul era *z*, discul folosit putea fi *4*, *5* sau *6*. Alegerea pentru celelalte litere este, de asemenea, limitată. Criptanalistul asamblează discurile bazîndu-se pe aceste alegeri şi, deoarece mesajul a fost cifrat cu douăzeci de litere o dată, încearcă descifrări la intervale de cîte 20 de litere. Dacă apar atoli clari în marea de cifruri, este clar că a găsit permutarea exactă a cîtorva discuri şi poate, prin anagramă, să mărească aceste insuliţe într-un arhipelag şi, în cele din urmă, să le unească într-un continent de text clar. Dacă nu apare nici un fel de text clar, criptanalistul trebuie să continue căutarea prin criptogramă pînă apare o altă posibilitate. În cazul în care nici o astfel de posibilitate nu apare cu echivalenţi de pe primul generatrix, criptanalistul trebuie să încerce cu a doua şi aşa mai departe.

„Întregul proces — zicea de Viaris — cere mai mult timp pentru a fi explicat decît aplicat".

În ciuda acestei excelente criptanalize, Bazeries nu a vrut să recunoască că de Viaris făcuse ceea ce el făcea de obicei : găsise o soluţie valabilă pentru cilindrul lui.

Respingerea cilindrului nu l-a liniştit pe Bazeries, căruia îi era teamă că slăbiciunea cifrurilor militare pun în pericol Franţa, dar şi celelalte sisteme ale sale au fost respinse, deşi unul, care avea o cheie formată pe baza a două litere, n-a fost soluţionat niciodată de criptanaliştii armatei franceze.

Cheia era formată din două litere transformate într-un număr după regula $A = 1$, $B = 2$ şi aşa mai departe. Acest număr scris în cuvinte forma alfabetul de cifrat. Folosind alfabetul englez, *SF* devenea *186* sau ONE HUNDRED EIGHTY-SIX, dînd ca alfabet cheia O N E H U N D R I G T Y S X A B C F J K L M Q U W Z. După ce textul clar era substituit cu ajutorul acestui alfabet, criptograma era împărţită în grupe de cîte trei litere în care se inversa ordinea. Se puteau, de asemenea, interpola vocale şi nule pentru a întări sistemul, iar cheia se schimba pentru fiecare mesaj.

Toate aceste invenţii în domeniul criptografiei se făceau pentru armată. Întreaga Europă care se pregătea de război era cuprinsă de febra criptologică. Ea voia să fie bine pusă la punct în această privinţă.

Războiul avea să dovedească justeţea celor care şi-au asigurat din timp un arsenal criptologic. Acesta i-a ajutat să dobîndească multe victorii şi să contracareze multe acţiuni inamice.

„CAMERA 40"

În ziua de 5 august 1914, prima zi a războiului care avea să cuprindă ţară după ţară, o navă încărcată cu echipament special aluneca încet pe apele plumburii ale Mării Nordului. În apropiere de Emden, locul unde se învecinează Olanda şi Germania, a fost aruncat spre adîncimi un cîrlig cu ajutorul căruia au fost ridicate pe bord cablurile transatlantice care făceau legătura dintre Germania şi restul lumii. O simplă lovitură de bardă şi cablurile au căzut înapoi în mare, complet nefolositoare.

Din acel moment, Germania a fost nevoită să comunice cu străinătatea prin radio sau prin linii telefonice controlate de inamic. În felul acesta, ea dădea duşmanilor săi posibilitatea de a-i cunoaşte cele mai secrete planuri şi intenţii, bineînţeles, dacă aceştia erau în stare să înlăture păienjenişul de cifruri şi coduri care le ascundeau. Era o situaţie pentru care englezii nu erau pregătiţi, dar n-au vrut să lase să le scape ocazia de a obţine informaţii.

În acest sens, s-au luat măsuri de înfiinţare a unui birou special care se ocupa cu decriptarea mesajelor interceptate de la inamic şi în fruntea căruia a fost pus sir Alfred Ewing. Totuşi, activitatea în acest birou a demarat destul de greu, englezii, la vremea aceea, fiind destul de ageamii în ce priveşte secretele criptologiei. În schimb, le-a surîs norocul! La începutul lunii septembrie 1914, crucişătorul german Magdeburg

a fost distrus pe cînd se afla în Marea Baltică. Cîteva ore mai tîrziu, ruşii au pescuit din apele mării cadavrul unui subofiţer german. Asupra acestuia s-au găsit cifrul şi tabelul de semne şi semnale ale marinei de război germane. Ruşii, considerînd că aceste documente prezentau interes pentru Anglia, pe atunci cea mai mare putere maritimă, au cerut ca o navă britanică să meargă la Petrograd ca să ia în primire preţioasa pradă de război. Cu toate că aveau cifrul, englezilor le-a mai trebuit o perioadă de timp pînă să reuşească să decripteze primele mesaje interceptate. Principala piedică o constituia supracifrarea monoalfabetică folosită de nemţi, deşi soluţia unei asemenea supracifrări nu este prea dificilă, mai ales cînd ai cifrul. Ca şi în textul clar, anumite simboluri din cadrul textului cifrat sau codificat se întîlnesc mai des decît altele. Uneori, anumite cuvinte codificate se repetă după o anumită structură. În cazul codului german, consoanele alternau cu vocalele în grupe de cîte patru litere. Cînd se cunosc aceste lucruri, criptanalistul le remarcă imediat şi le foloseşte pentru a soluţiona supracifrarea.

Trei săptămîni le-au trebuit englezilor pînă au reuşit să descifreze frînturi din mesajele interceptate de la nemţi.

Între timp, Ewing a reuşit să încadreze un număr mare de criptologi, iar acest serviciu a primit denumirea sub care avea să fie cunoscut de toată lumea : „Camera 40".

În urma descifrării ordinului transmis unei flotile din marina de război germană de a bombarda cîteva porturi britanice, Amiralitatea britanică a elaborat un plan prin care cîteva din cele mai puternice nave de război engleze au fost dirijate în zona prin care urma ca respectiva flotilă să se reîntoarcă în Germania. Succesul a fost deplin. Timp de un an de zile, germanii n-au mai putut părăsi porturile din Marea Nordului, deoarece majoritatea navelor fuseseră avariate sau distruse, iar echipajele suferiseră pierderi grele.

Între timp, germanii au schimbat cheia de supracifrare, dar englezilor, care de acum căpătaseră o oarecare experienţă şi învăţaseră meserie, le-a fost necesară doar o noapte pentru a înţelege mesajele şi ordinele transmise de nemţi prin radio.

O caracteristică a perioadei respective o constituia faptul că nemţii dădeau mare atenţie războiului submarin. Cu toate acestea, în ciuda multelor măsuri de securitate pe care le luau, nu de puţine ori submarinele lor erau interceptate.

În cele din urmă au bănuit că englezii deţin codul şi atunci au hotărît să-l schimbe. Aşa se face că, în luna august 1916, pe întreaga flotă germană a fost schimbat codul. Dar la acea dată „Camera 40" era atît de versată în decriptări încît Amiralitatea britanică nu a simţit lipsa informaţiilor provenite din această sursă. Curînd după aceea, parcă pentru a verifica justeţea soluţiilor găsite de criptanaliştii „Camerei 40", a fost recuperat de pe nava germană „Zeppelin L-32" noul cod german, care a fost trimis la Amiralitatea britanică. Criptanaliştii şi-au dovedit clasa şi valoarea, iar codul respectiv i-a ajutat să facă faţă în condiţii de operativitate sporită numărului din ce în ce mai mare de mesaje interceptate.

Pe măsură ce numărul de mesaje interceptate sporea, creştea şi personalul „Camerei 40". Calitatea deosebită a acestui personal o dovedeşte faptul că, după război, majoritatea celor care au lucrat în „Camera 40" au devenit profesori universitari, doctori în ştiinţe, oameni de litere şi critici literari remarcabili. În acest sens, este ilustrativ faptul că pînă şi dactilografele, pentru a putea lucra la acest serviciu, trebuiau să cunoască cel puţin două limbi străine. Pe baza informaţiilor primite de la „Camera 40", flota britanică a reuşit să distrugă majoritatea navelor de război germane. „Camera 40" a funcţionat pe tot timpul primului război mondial şi unul din cele mai mari succese l-a înregistrat în anul 1917. Acest succes merită să fie relatat, mai ales că el ilustrează rolul criptologiei în desfăşurarea evenimentelor istorice.

În dimineaţa zilei de 17 ianuarie 1917, reverendul William Montgomery, care lucra în calitate de criptanalist la secţia diplomatică a „Camerei 40", a prezentat primului lord al amiralităţii o criptogramă pe care el o considera importantă.

Criptograma era destul de mare ca întindere, fiind formată din mai mult de o mie de grupe numerice. Datată la Berlin pe

16 ianuarie, ea era adresată ambasadorului german acreditat în Statele Unite ale Americii.

Montgomery și colegul său, Nigel de Grey, și-au dat seama că mesajul era codificat pe baza unui cod diplomatic german cunoscut ca fiind codul 0075. Cei doi începuseră să acționeze asupra codului respectiv cu șase luni în urmă. Aflaseră că, în realitate, 0075 era una din seriile unui cod german construit din două zerouri și două cifre, între care exista întotdeauna o diferență aritmetică de două unități. Printre celelalte serii soluționate de „Camera 40" erau seriile 0097 și 0086, folosite de Ministerul de Externe german în corespondența cu reprezentanțele sale diplomatice acreditate în țările Americii Latine. A fost soluționată, de asemenea, seria 0064, folosită în corespondența dintre Berlin și Madrid. Seria 0075, întocmită în 1916 și difuzată misiunilor diplomatice germane de la Viena, Sofia, Constantinopole, București, Copenhaga, Stockholm, Berna, Lugano, Haga și Oslo, nu fusese încă soluționată, dar englezii reușiseră să intercepteze un număr destul de mare de telegrame ca să o poată ataca. Montgomery și de Grey au primit misiunea de a o ataca și soluționa.

La 17 ianuarie 1917, Montgomery și de Grey puteau citi doar unele părți ale mesajului pe care l-au primit în dimineața aceea, dar chiar din cît au putut citi și-au dat seama de importanța lui, căci au decriptat semnătura ministrului de externe german Arthur Zimmermann. Ceea ce puteau ei citi, pe baza a ceea ce reușiseră să cunoască din Codul 0075, suna cam așa :

„Secret de importanță deosebită ! Numai pentru informarea Excelenței Voastre, care să ia măsuri ca acest mesaj să fie înmînat ministrului nostru plenipotențiar (din Mexic ?) împreună cu telegrama nr. 1 (...) pe o cale sigură.

Ne propunem ca, de la întîi februarie, să începem un război submarin total. Se pune problema ca să ne asigurăm de neutralitatea Statelor Unite (?) Dacă nu vom reuși (să determinăm S.U.A. să rămînă neutră ?), vom propune (Mexicului ?) o alianță pe următoarea bază :

...ducerea (în comun ?) a războiului;
...încheierea păcii (de comun acord ?):
(..)

Excelența Voastră trebuie, pe această bază, să informeze pe președinte (al Mexicului ?) în mod secret că noi ne așteptăm la un război cu S.U.A. (posibil ?) (...) (Japonia) și, în același timp, să negocieze între noi și Japonia. Vă rog să-i spuneți președintelui că (...) sau submarinele (...) vor forța (obligat ?) Anglia să ceară pace în cîteva luni. Confirmați primirea.

Zimmermann"

Montgomery a înaintat acest fragment din textul cifrat lui Hall, șeful serviciului de informații navale, căruia i se subordona și „Camera 40".

Hall a privit la cuvintele din mesaj și a înțeles imediat că era de o importanță deosebită. A ordonat lui Montgomery să facă totul pentru a-l decripta în întregime, iar copiile să fie arse. Apoi, fără nici un alt cuvînt, a plecat la Ministerul de Externe ca să mediteze asupra situației.

Războiul despre care toată lumea crezuse că o să se termine în cîteva săptămîni dura de aproape trei ani. Pierderile, mai ales în vieți omenești, erau uriașe. Într-o singură zi, englezii pierduseră pe Somme 60 000 de soldați și reușiseră să înainteze doar cîțiva zeci de metri. Nu se întrevedea nici un sfîrșit acestui război.

Situația Germaniei nu era mai bună. În ciuda inițiativei din prima parte a războiului, succesele se lăsau așteptate, iar trupele nemțești se îngropaseră în tranșee unde păreau că o să putrezească. Singura cale de a ieși din această situație era războiul submarin. „Dați-ne voie să declanșăm un război submarin total și în curînd Anglia se va zbate ca peștele pe uscat" spuneau generalii nemți. Cum rezultatele de pe front erau din ce în ce mai nesatisfăcătoare, cei care se opuseseră cu vehemență unui război submarin total au început să dea înapoi. Zimmermann, care făcuse și el parte dintre opozanți, și-a dat seama că scufundarea vaselor americane va torpila neutralitatea S.U.A. și, de aceea, încerca să încheie o alianță cu Mexicul.

Neavînd posibilitatea de a trata această propunere cu ambasadorul Mexicului, deoarece acesta își avea reședința în Elveția, Zimmermann a hotărît să negocieze prin ambasadorul german din Mexic, Heinrich von Eckardt. Pentru a transmite mesajul respectiv avea două posibilități, ambele controlate însă de englezi. Una din aceste posibilități era oferită de Suedia, care, deși neutră, era favorabilă Germaniei. Guvernul suedez transmitea mesajele germane ca fiind propriile sale mesaje. Totuși, întrucît cablul transoceanic suedez atingea țărmurile Angliei, nemților le era teamă că englezii vor recunoaște cifrurile lor. Atunci au recurs la mascarea lor, supracifrîndu-le. Dar supracifrarea n-a reușit să ascundă în întregime caracterul codului folosit și unele caracteristici au atras atenția criptanaliștilor englezi. După ce au înlăturat cheia de supracifrare a apărut la suprafață codul 13040. Din acel moment, „Camera 40“ a acordat o atenție deosebită mesajelor și telegramelor suedeze.

A doua cale folosită de Zimmermann era foarte îndrăzneață și își avea originea în aranjamentul făcut de colonelul american Edward House, consilierul președintelui Wilson. În timpul unei misiuni în Europa, House a fost de acord ca guvernul german să trateze problemele de interes comun pentru S.U.A. și Germania direct cu președintele Wilson, trecîndu-se peste Departamentul de Stat. În acest sens, s-a permis germanilor să trimită mesaje codificate cu propriul lor cod la Washington sub protecția americană și prin intermediul mijloacelor de comunicație de care dispuneau aceștia.

Americanii îi protejau pe inamicii proprii, însă trimiteau mesajele lor din Europa în S.U.A. prin Copenhaga și Londra, iar englezii au fost „încîntați“ să recunoască printre telegramele americane și pe cele nemțești — codificate.

Avînd deci două copii ale telegramei în coduri diferite, Montgomery și Grey au atacat textul cu deosebită vigoare.

Totuși, soluția la telegrama lui Zimmermann cerea mai mult decît o clipă de respirație. Pentru soluționare era necesar să fie reconstituit codul 0075, cod ce însuma 10 000 de cuvinte și expresii substituite în grupuri de cifre de la 0000 la 9999.

Deoarece un cod nu este altceva decît o substituție monoalfabetică gigantică, stabilirea echivalenților este „singura“ greutate. Dar dacă criptanalistul de cifru are de-a face doar cu 26 asemenea elemente, criptanalistul de cod are de-a face cu sute și mii de elemente ale căror caracteristici sînt foarte greu de descoperit.

Soluția, de obicei, începe prin identificarea grupelor care ascund cuvîntul *stop*. De asemenea, grupele de la sfîrșitul telegramelor sînt atacate cu prioritate. Identificarea lui *stop* sau *pauză* este ușurată de faptul că se folosesc, de obicei, puțini echivalenți. O dată identificat cuvîntul *stop* se are în față structura mesajului. În engleză substantivele, fiind subiectul propozițiilor, apar imediat după cuvîntul *stop*. În germană, predicatul sau verbul este aproape întotdeauna la sfîrșitul propoziției, precedînd cuvîntul *stop*. Alte date se extrag din expresiile stereotipe care se folosesc, mai ales de diplomați, în toate mesajele. De exemplu: „Am onoarea să raportez Excelenței Voastre...“. Informațiile colaterale sînt, de asemenea, de o foarte mare valoare și importanță.

Prima tentativă se scrie în creion pentru a putea fi ștearsă. Apoi grupele care se verifică se scriu cu cerneală. Dacă codul e simplu, atunci soluția apare destul de repede. Dacă, de exemplu, 1234 reprezintă un cuvînt ce începe cu litera *d*, atunci 5678 va reprezenta un cuvînt care începe cu o literă aflată după *d* în alfabet etc. Astfel de prezumții ajută la identificări. Cîteodată, dacă o grupă este situată între alte două grupe cunoscute, atunci ne putem aventura să-i ghicim înțelesul. Dar acest lucru nu-i posibil cînd avem cod dublu, unde ordinea nu mai are nici un fel de importanță, dominînd arbitrarul în substituție. Codul 0075 era de acest gen. Erau necesare cît mai multe mesaje codificate cu ajutorul lui pentru a se putea stabili care erau substituțiile. Cum acesta era folosit doar de o jumătate de an — durată mică de folosire pentru un cod diplomatic — multe pasaje din diferite telegrame în care a fost folosit au rămas nerezolvate.

Dar zi și noapte apăreau noi telegrame. Montgomery și Grey, lucrînd pînă la epuizare, rezolvau noi grupuri, din ce în

ce mai rapid. La 28 ianuarie, de Grey i-a adus lui Hall un protest al lui Bernstoff, ambasadorul german în S.U.A., împotriva planului lui Zimmermann de a declanşa un război submarin total. Bernstoff se pronunţa cu hotărîre împotriva acestui plan, deoarece îşi dădea seama că punerea lui în aplicare ar fi însemnat torpilarea eforturilor pe care el le depunea în vederea unei destinderi între S.U.A. şi Germania, fapt care ar fi împiedicat intrarea Statelor Unite în război de partea Antantei.

La 3 februarie, Wilson, preşedintele S.U.A., a anunţat Congresul că va rupe relaţiile diplomatice cu Germania dacă aceasta va declanşa un război submarin total, dar preciza că va face acest lucru doar în cazul în care „faptele vor arăta că nemţii scufundă în mod deliberat vasele ţărilor neutre ce navighează în apele internaţionale".

În timp ce preşedintele S.U.A. aştepta „faptele", „Camera 40" îşi continua activitatea soluţionînd codul 0075. De Grey a mai reuşit, cunoscînd din alte surse conţinutul convorbirii ce a avut loc între Wilson şi Bernstoff, să soluţioneze şi alte grupuri din codul respectiv. Făcînd substituţiile care se impuneau, la 5 februarie de Grey era în măsură să descifreze aproape în întregime telegrama lui Zimmermann.

Hall apreciase încă din prima zi că această telegramă reprezenta o valoare de proporţii deosebite. Demascarea publică sau pe canale diplomatice a intenţiilor Germaniei, care aduceau o atingere directă intereselor S.U.A., în condiţiile date, obligau guvernul american să declare război Imperiului German. În acest sens, telegrama era o dovadă evidentă care trebuia prezentată fără întîrziere americanilor, dar, pentru moment, motive mai puternice îi opreau pe englezi s-o facă. Primul motiv era acela că existenţa „Camerei 40" şi posibilităţile de criptanaliză ale serviciului secret britanic constituiau unul dintre cele mai importante secrete ale Angliei. Cum se putea, totuşi, folosi această informaţie fără ca nemţii să afle cum reuşiseră englezii să intre în posesia ei ? Se putea spune că telegrama fusese furată, dar exista pericolul ca nemţii să bănuiască adevărul şi să schimbe codul. În al doilea rînd, dacă englezii arătau telegrama se autodemascau că interceptaseră

cablul transoceanic al unei ţări neutre — Suedia. În acest caz, nu era nevoie de prea multă isteţime ca americanii să-şi dea seama că şi corespondenţa lor era interceptată. Această constatare n-ar fi dus în nici un caz la o simpatie a americanilor faţă de Anglia şi faţă de Antantă, în general. În al treilea rînd, telegrama nu fusese descifrată în întregime. Părţile nesoluţionate din telegramă ar fi ridicat semne de întrebare asupra corectitudinii descifrării, deoarece se putea foarte bine ca englezii să nu fi reuşit să soluţioneze o negaţie, care ar fi schimbat complet sensul telegramei. De asemenea, porţiunile nesoluţionate ar fi arătat clar că era vorba de decriptarea unei telegrame şi nu de sustragerea ei. Dar cel mai puternic motiv împotriva folosirii telegramei era acela că timpul lucra în favoarea Antantei, deoarece americanii adoptau cu fiecare zi ce trecea o poziţie tot mai ostilă faţă de Germania. În aceste condiţii, Anglia aştepta şi spera.

Hall n-a rămas, totuşi, în expectativă. El considera că nu-şi făcea datoria din moment ce nu putea pune la dispoziţia guvernului britanic, pentru a o folosi în interesul ţării, soluţia telegramei lui Zimmermann.

În consecinţă, a conceput un plan care, dintr-o singură lovitură, înlătura trei din motivele care îi împiedicau pe englezi să se folosească de telegramă.

Întrucît telegrama fusese trimisă mai întîi la Washington, unde a fost recodificată în alt cod de către ambasadorul german de aci pentru a fi transmisă mai departe în Mexic, era uşor de presupus că ea suferise unele mici modificări de formă, cum ar fi : schimbarea datei expedierii ei şi preambulul. Deci, dacă Hall putea să facă rost de copia acestei telegrame, atunci automat nemţii ar fi presupus că cineva din Mexic trădase şi n-ar fi schimbat codul folosit în Europa. Alte fapte puteau lăsa impresia că era vorba de o sustragere a telegramei din ambasada germană din Mexic. „Camera 40" ştia bine că, în corespondenţă, ambasada germană din Mexic nu folosise niciodată codul 0075, acesta fiind şi faptul care l-a determinat pe Hall să creadă că Bernstoff recodificase telegrama lui Zimmermann

într-un cod care, n-ar fi fost de mirare, să fi fost soluționat cîndva de englezi.

Începînd cu 5 februarie, Hall a ordonat să se caute cu insistență o copie a telegramei așa cum a ajuns ea în Mexic. Un agent englez, cunoscut doar după inițiala „T", a obținut de la oficiul telegrafic din Mexic o copie a mesajului lui Bernstoff către Eckardt.

Toate prezumțiile făcute s-au confirmat. Eckardt nu avea codul 0075, așa că telegrama fusese recodificată, iar codul folosit nu era altul decît codul 13040, un cod mai vechi și mai ușor de soluționat decît 0075. Codul 13040, distribuit misiunilor diplomatice germane din țările latino-americane, conținea 250 000 de elemente clare și un număr destul de mare de homofone — numai în telegrama lui Bernstoff se foloseau șase grupuri de cifre diferite pentru *zu*, iar numele proprii aveau peste 75 000 de echivalenți. Dar codul 13040 era o combinație între un sistem de cod simplu și unul dublu. În partea de cod, grupurile de echivalenți aranjate în ordine numerică crescîndă erau opuse elementelor clare aflate în ordine alfabetică. Spre ilustrare, dăm cîteva secțiuni din cod :

13605	Februar	4377	geheim
13732	fest	4458	Gemeinsame
13850	finanzielle	5144	wenigen
13918	folgender	5161	werden
17142	Frieden	5275	Anregung
17149	Friedenschluss	5376	Anwendung
17166	führung	5454	ar
17214	Ganz geheim	5569	auf
17388	Gebeit	5905	Krieg

Soluționarea unui astfel de cod hibrid este mai ușoară decît rezolvarea unui cod complex și mai grea decît cea a unui cod simplu. Ordinea numerică crescîndă din grupurile respective îl ajută mult pe criptanalist, dar ghicitul nu mai este atît de sigur ca în cazul codului simplu. De exemplu, criptanalistul

nu poate spune că cifra care reprezintă cuvîntul Krieg este un număr mai mare decît cel care-l reprezintă pe Februar. Dar, dacă a aflat că Februar = 13605 și finanzielle este 13850, atunci pentru el e clar că fest este reprezentat de un număr aflat între cele două. Identificările, în acest caz, sînt mai rapide și mai sigure.

Datorită acestei slăbiciuni, cît și faptului că în timpul războiului criptanaliștii „Camerei 40" soluționaseră un mare volum de mesaje, codul 13040 a fost refăcut aproape în întregime. Folosind procedeele menționate, ei au reușit să descifreze o mare parte din mesajul lui Bernstoff către Eckardt, iar acolo unde au întîlnit nume proprii sau silabe folosite pentru prima oară, aranjamentul alfabetic le-a asigurat o premisă sigură pentru ghicit. În plus, acest lucru a confirmat încă o dată că soluția adoptată pentru descifrarea mesajului original dintre Berlin și Washington a fost bine aleasă și s-au făcut noi pași în direcția soluționării depline a codului 0075.

Tot cu această ocazie s-au adeverit și presupunerile lui Hall. Bernstoff înlocuise preambulul Ministerului de Externe german cu unul personal.

De asemenea, mesajul purta data de 19 ianuarie, în loc de 16 cît era în original, iar numărul de serie dat de Berlin era înlocuit cu unul propriu.

În februarie, Hall era gata de acțiune. Ideea lui genială avea să dea roade. Această acțiune de conspirare a sursei de unde provenise informația este una dintre cele mai subtile. Acum era posibil ca telegrama să fie dată americanilor cu foarte puține riscuri de desconspirare a surselor de informații ale serviciului secret. Deși ștersese urmele, Hall nu s-a grăbit totuși să transmită americanilor informația și a hotărît să mai aștepte să vadă cum evoluează evenimentele. Aceasta cu atît mai mult cu cît președintele american, deși nemții le torpilau vapoarele, nu părea să fie gata să intre în acțiune. El aștepta „faptele" care să-i dovedească că nemții torpilau în mod premeditat navele de transport americane. În cele din urmă, cum nemții se străduiau din răsputeri să nu le furnizeze asemenea „fapte" incriminatorii, iar situația de pe front se înrăutățea

continuu, la 22 februarie 1917, Hall, cu aprobarea Ministerului de Externe, a arătat lui Edgard Bell, secretarul ambasadei americane la Londra, care ţinea legătura cu serviciul secret britanic, textul clar al telegramei lui Zimmermann. Bell a citit uimit următoarele :

„Noi intenţionăm să începem, de la 1 februarie, războiul submarin total. Sîntem interesaţi să ne asigurăm de neutralitatea S.U.A. În eventualitatea că nu vom reuşi acest lucru, facem Mexicului propunerea de a încheia cu noi o alianţă şi de a duce războiul împreună. În acest caz, Mexicul va beneficia de un ajutor financiar generos din partea noastră şi va primi, după obţinerea victoriei, teritoriile pierdute din Texas, New Mexico şi Arizona.

Am dori ca preşedintele Mexicului să ia de urgenţă cunoştinţă despre cele de mai sus şi-l rugăm să intervină pe lîngă Japonia să ni se alăture.

Rugăm, de asemenea, ca preşedintele mexican să fie convins că recurgerea la războiul submarin total oferă perspectiva înfrîngerii Angliei în cîteva luni.

Zimmermann"

Lui Bell nu-i venea să creadă, dar Hall l-a convins de autenticitatea telegramei şi, împreună, au plecat la ambasada americană. Ambasadorul american şi-a dat seama că acest document era egal cu intrarea S.U.A. în război şi, împreună cu Hall, Bell şi Irwin Laughlin, primul secretar al ambasadei americane, şi-au bătut capul o zi întreagă căutînd cele mai bune căi prin care să insufle încredere în conţinutul telegramei şi să reducă la minimum orice îndoială asupra autenticităţii ei. S-a hotărît ca guvernul britanic să înmîneze oficial telegrama ambasadorului S.U.A. şi, în ziua următoare, Arthur Balfour, ministrul de externe englez, într-un cadru oficial şi, în acelaşi timp, dramatic, i-a înmînat telegrama lui Page.

Page a lucrat o noapte la legenda care urma să conspire modalitatea în care fusese obţinută telegrama. La ora două noaptea, el a telegrafiat în S.U.A. că va trimite preşedintelui acestei ţări şi secretarului de stat o telegramă de importanţă deosebită.

Legenda care însoţea telegrama era următoarea :

„În prima parte a războiului, guvernul britanic a intrat în posesia unei copii a codului folosit în mesajul pe care vi-l trimitem şi s-a preocupat în mod deosebit ca să obţină şi altele de acest gen de pe telegramele trimise de Bernstoff în Mexic. Aşa au reuşit criptanaliştii englezi să descifreze telegrama trimisă de guvernul german reprezentantului său în Mexic. Tot acesta este şi motivul care explică intrarea atît de tîrziu în posesia informaţiei de faţă.

Sursa aceasta de informaţii a fost conspirată cu deosebită grijă. Acum este prima dată cînd guvernul britanic, luînd în consideraţie condiţiile deosebite şi sentimentele lui de prietenie faţă de S.U.A., încalcă normele pe care şi le-a propus şi face această desconspirare faţă de o altă ţară. Guvernul britanic roagă insistent să se ţină strict secretă sursa de obţinere a informaţiei, dar nu se opune publicării în presă a telegramei".

Indignaţi de neruşinarea cu care nemţii se folosiseră de privilegiile acordate de S.U.A. în domeniul folosirii mijloacelor de comunicaţie americane, yankeii s-au pus în mişcare. În ziua de 1 martie telegrama a fost dată publicităţii şi a avut efectul scontat. Totuşi, unii congresmeni se întrebau dacă nu-i cumva vorba de o maşinaţiune din partea ţărilor Antantei. Atunci, secretarul de stat al S.U.A. a făcut rost de o copie a telegramei lui Bernstoff către Eckardt şi a trimis-o la Londra lui Page cu următoarea notă :

„Unii membri ai Congresului încearcă să pună sub semnul întrebării autenticitatea telegramei lui Zimmermann, acuzîn-

du-ne că am primit-o de la o țară beligerantă. Guvernul nostru nu are nici cea mai neînsemnată îndoială în acest sens, dar ni s-ar face un mare serviciu dacă guvernul britanic ar permite cuiva de la ambasada noastră să descifreze cu ajutorul codului german textul telegramei codificate procurat de către noi de la oficiul telegrafic din Washington și să ne telegrafieze rezultatul. Asigurați-l pe dl Balfour că Departamentul de Stat a ezitat să-și exprime această dorință, dar credem că prin aceasta ne creăm posibilitatea materială să declarăm că noi singuri, prin proprii noștri funcționari, am reușit să cunoaștem conținutul telegramei".

A doua zi, Page telegrafia la Washington : „Bell a luat textul cifrat și s-a dus la Amiralitate, unde l-a descifrat cu ajutorul codului care se află în posesia Marinei regale". În realitate, Bell n-a făcut prea mare lucru, ci de Grey a fost cel care a făcut decriptarea.

Președintele S.U.A. și secretarul de stat au declarat în Congres că telegrama era autentică și că, din motive de securitate, nu se pot da și alte detalii. A fost lăsat fiecare să creadă ce dorește în legătură cu modul în care guvernul american a intrat în posesia telegramei. Cei mai mulți credeau că era vorba de reușita unui spion. Alții spuneau că patru soldați americani au găsit-o asupra unui agent german care voia să treacă granița în Mexic. Foarte plauzibil era și zvonul că ar fi fost găsită printre efectele lui Bernstoff, cînd acesta a fost nevoit să părăsească S.U.A. Cele mai amuzante erau însă atacurile presei britanice care criticau ineficacitatea propriului serviciu secret și scoteau în relief inferioritatea lui față de cel american. (Cel puțin unul dintre aceste atacuri a fost inițiat de Hall ca să-și scoată serviciul său din cauză).

Berlinul își făcea probleme, căutînd să afle unde s-a produs scurgerea. Eckardt, tremurînd, dădea cele mai impresionante detalii ca să se disculpe : „Ambele mesaje primite au fost descifrate, în conformitate cu instrucțiunile pe care le-am primit, de către Magnus, secretarul ambasadei. Nici unul, nici altul dintre ele, ca de altfel toate mesajele de natură politică, nu au fost cunoscute de către ceilalți funcționari ai ambasadei... Originalele au fost arse de Magnus, iar cenușa a fost împrăștiată. Pînă la ardere, mesajele au fost ținute într-un seif sigur, procurat special pentru acest scop și instalat în dormitorul lui Magnus, aflat în clădirea ambasadei". Trei zile mai tîrziu, Eckardt transmitea și rezervele sale : „Mai multe măsuri de precauție decît cele luate aici sînt imposibile. Textele telegramelor îmi sînt citite cu voce joasă de Magnus în locuința mea. Servitorul, care nu înțelege germana, doarme într-o anexă... Nu poate fi vorba aici de hîrtia de indigo sau de alte copii". Hohotele de rîs stîrnite de acest răspuns în „Camera 40" n-au fost auzite la Berlin.

Între timp, problema autenticității telegramei, care a dat atîta bătaie de cap oficialităților anglo-americane și ridicase semne de întrebare în Congres și presă, a fost rezolvată de... Zimmermann în persoană. Cu totul pe neașteptate, acesta a declarat : „Nu pot să neg. Telegrama este autentică". Mexicanii și japonezii au negat că ar fi știut ceva de această acțiune și, pînă astăzi, nimeni nu știe de ce Zimmermann a recunoscut că telegrama îi aparținea.

La 2 aprilie, Wilson, care cu trei luni mai devreme declarase că „este o crimă împotriva civilizației" ca S.U.A. să intre în război, a cerut Congresului aprobarea de a declara război Germaniei.

Citind telegrama lui Zimmermann, el a spus : „faptul că guvernul german încearcă să ne creeze dușmani chiar lîngă granița noastră este dovedit de nota către ministrul german din Mexico City, de aceea propun Congresului să declare că acceptă

provocarea şi declarăm că acţiunile întreprinse de guvernul german nu sînt altceva decît operaţiuni de război împotriva poporului Statelor Unite".

Aşa se face că soluţia găsită de „Camera 40" unei telegrame trimisă de inamic a permis grăbirea intrării S.U.A. în război şi, în final, cîştigarea lui.

RĂZBOIUL INTERCEPTĂRILOR

Cînd a izbucnit războiul, din punctul de vedere al criptologiei numai Franţa era pregătită. În acel moment, secţia criptologică a Ministerului de Război francez primise personal nou, iar staţiile de interceptare se înmulţiseră. „Francezii — a declarat Cartier, şeful secţiei criptologice — au interceptat în timpul războiului mai mult de 100 000 000 de cuvinte sau mesaje care ar forma o bibliotecă de 1 000 de romane de grosime medie".

Ei au reuşit să spargă cifrul german ÜBCHI, bazat pe o transpoziţie pe două coloane şi o cheie care, înainte de cifrare, era transformată într-o secvenţă numerică. Această operaţie se făcea dînd valori numerice literelor din cheie, luate în ordine alfabetică. În cazul în care unele litere se repetau, fiecare dintre ele primea o altă valoare numerică ce creştea de la stînga la dreapta. Dacă luăm ca exemplu cheia DIE WACHT AM RHEIN, cei doi *A* primeau numerele *1* şi *2*. *B* nu este, aşa că *C* primea numărul *3*, *D* numărul *4*, cei doi *E 5* şi *6* şi aşa mai departe.

DIE WACHT AM RHEIN
495 1513714 211 13861012

Cifrarea unui text clar, să spunem: Tenth division X attack Montigny sector at daylight X. Gas barrage to precede you[1] implică şase etape separate.

[1] În limba română: „Divizia a zecea X atacă sectorul Montigny în zorii zilei X. Va fi precedată de un baraj de gaze".

1. Cifrorul scrie textul clar orizontal sub formă de tabel sub secvența de numere din cheie :

4	9	5	15	1	3	7	14	2	11	13	8	6	10	12
t	e	n	t	h	d	i	v	i	s	i	o	n	x	a
t	t	a	c	k	m	o	n	t	i	g	n	y	s	e
c	t	o	r	a	t	d	a	y	l	i	g	h	t	x
g	a	s	b	a	r	r	a	g	e	t	o	p	r	e
c	e	d	e	y	o	u								

2. Transcrie literele din coloane în ordinea naturală a numerelor care formează cheia : HKAAY, ITYG, DMTRO și așa mai departe.

3. Le transcrie orizontal în alt tabel sub aceeași cheie.

4. În tabelul obținut mai adaugă exact același număr de nule cîte cuvinte se găseau în expresia care formează cheia originală, în cazul nostru patru :

4	9	5	15	1	3	7	14	2	11	13	8	6	10	12
h	k	a	a	y	i	t	y	g	d	m	t	r	o	t
t	c	g	c	n	a	o	s	d	n	y	h	p	i	o
d	r	u	o	n	g	o	l	t	t	a	e	x	s	t
r	s	i	l	e	a	e	x	e	i	g	i	t	v	n
a	a	t	c	r	b	e	k	a	i	s				

5. Cifrorul retranscrie coloanele în șiruri orizontale în ordinea literelor din cheie : YNNER, GDTEA, IAGAB etc.

6. Șirurile obținute sînt împărțite în grupe de cîte cinci litere pentru a fi transmise :

YNNER GDTEA IAGAB HTDRA AGUIT RPXTT OOEET HEIKC RSAOI SVDNT IITOT NMYAG SYSEX KACOL C.

Descifrarea este procesul invers al cifrării, criptanalistul trebuind să determine mărimea careului de transpoziție pentru

a putea ști cît de mari sînt coloanele. Acest fapt se poate obține împărțind numărul total al literelor la numărul literelor din cheie, în cazul nostru 71 la 14. Se obțin astfel 4 rînduri complete și un rînd incomplet de 11 litere.

Soluționarea unui singur mesaj cifrat prin transpoziție dublă este o problemă extraordinar de grea. Pentru a ne da seama de aceasta, exemplificăm cu ajutorul unei transpoziții simple. Criptanalistul va începe prin a împărți criptograma în ceea ce consideră el că ar putea fi coloanele și apoi juxtapune segmentele între ele pînă găsește două care ar putea sta unul lîngă altul în tabelul original.

Să luăm o criptogramă de 40 de litere. Criptanalistul presupune că cheia este formată din cinci litere. Coloanele vor fi formate din opt litere, iar criptanalistul va împărți criptograma în grupe de cîte opt litere și va împerechea primul grup cu celelalte patru :

1—2	*1—3*	*1—4*	*1—5*	*2—1*	*3—1*	*4—1*	*5—1*
E N	E Y	E M	E E	N E	Y E	M E	E E
I H	I T	I R	I T	H I	T I	R I	T I
T E	T R	T H	T I	E T	R T	H T	I T
T G	T S	T I	T E	G T	S T	I T	E T
I R	I G	I N	I B	R I	G I	N I	B I
G N	G P	G U	G I	N G	P G	U G	I G
M M	M N	M U	M A	M M	N M	U M	A M
I T	I N	I O	I I	T I	N I	O I	I I

Aceste coloane pot fi analizate atît din vedere cît și cu ajutorul diferitelor metode matematice pentru a vedea care coloane merg cel mai bine împreună. O metodă constă în a stabili frecvența fiecărei bigrame dintr-un text clar, după care se face suma lor. Combinația care deține numărul cel mai mare este foarte probabil să fie cea bună. Astfel, *EN*, din împe-

recherea 1—2, are o frecvență normală de 25% (din 2 000 de bigrame în engleză). IH, zero și așa mai departe. Toate cele opt bigrame totalizează suma de 69. Celelalte combinații dau 73, 143, 77, 77, 73, 62 și 78. Criptanalistul va alege deci coloana 1—4 cu totalul 143, apoi încearcă să extindă bigramele în trigrame atît la stînga cît și la dreapta, prin aceeași metodă pînă cînd reconstituie întregul tabel.

Dacă rezultatul este nesatisfăcător, modifică prezumția originală și începe de la început întreaga operație.

Acest proces este simplificat dacă tabelul e complet. Cînd tabelul e complet se spune că avem transpoziție regulată, iar cînd tabelul este incomplet avem transpoziție neregulată.

Acest tip de reconstrucție este posibil numai în cazuri excepționale pentru transpoziții duble. În teorie, criptanalistul trebuie să construiască coloanele celui de-al doilea tabel și să afle bigramele și trigramele care să se transforme în text clar. Soluția însă devine relativ simplă cînd avem mai multe criptograme de aceeași lungime și cifrate cu aceeași cheie. Criptanalistul poate aplica atunci, pe baza literelor, metoda anagramării multiple folosită pentru cuvinte. De obicei, cele două mesaje sînt scrise unul sub altul pe fîșii de hîrtie, iar hîrtia este tăiată vertical, astfel încît două litere — cîte una din fiecare mesaj — se găsesc pe fiecare bucată de hîrtie și aceste bucățele se alătură una lîngă alta — căutînd ca ele să se potrivească — pînă cînd textul clar apare pe ambele șiruri. Metoda a dat rezultate și francezii căutau criptograme identice ca lungime și cheie pentru a le rezolva. Nemții le-au ușurat activitatea folosind o cheie 8—10 zile pe tot frontul de vest. Pe la sfîrșitul verii, mesajele interceptate cădeau pe birourile franțuzești ca frunzele toamna.

Succesele francezilor au fost deosebite. Ei au recunoscut și rezolvat, de asemenea, mesaje secrete scrise cu ajutorul grătarelor sau grilelor. Grătarul rotitor — cel mai des folosit — este un pătrat de hîrtie sau carton împărțit în căsuțe, dintre care unele sînt decupate. Decupajul se face astfel încît după ce grătarul a fost așezat în cele patru poziții pe un pătrat similar, în toate căsuțele din pătratul de dedesubt s-a putut scrie cîte o literă, fiecare căsuță fiind descoperită doar o singură dată.

Procedeul de criptare cu ajutorul grătarului este următorul : se așază grătarul peste pătratul de hîrtie similar și în căsuțele decupate se scriu literele mesajului pe care îl avem de transmis.

Apoi grătarul se întoarce cu nouăzeci de grade și se scriu în același mod literele următoare. Operația se repetă de încă două ori.

Cînd toate căsuțele din cel de-al doilea pătrat de hîrtie au fost completate, criptograful le poate transmite, citindu-le, de obicei, pe rînduri. Mesaje mai lungi se cifrează repetînd operația, iar dacă rămîn căsuțe goale, acestea se pot șterge sau umple cu nule.

Nemții au dat trupelor lor grătare de diferite mărimi. Fiecare avea un nume codificat după cum urmează : Anna — grătarul de 25, Berta — grătarul de 36, Clara — grătarul de 49, Dora — grătarul de 64, Emil — grătarul de 81 și Franz — grătarul de 100. Aceste nume codificate se schimbau săptămînal.

Sistemul grătarelor este în special susceptibil să fie soluționat prin metoda anagramării multiple, care este, în general, metoda de soluționare a sistemelor de cifrare prin transpoziție, deoarece secțiunile lor sînt obligatoriu de aceeași lungime. De asemenea, simetria lor a dat de gîndit și francezii au folosit și alte procedee pentru a le soluționa.

Aşa cum s-a văzut din capitolul precedent, precum şi din cel de faţă, criptologia a avut un rol deosebit în primul război mondial. Nemţii au neglijat acest aspect şi, în consecinţă, au avut de suferit multe înfrîngeri şi pierderi grele.

SECRETUL DE VÎNZARE

În decembrie 1917, Gilbert S. Vernam, un inginer american, lucra împreună cu un colectiv de cercetare la un proiect menit să găsească un mijloc pentru a asigura securitatea mesajelor transmise cu ajutorul teleimprimatoarelor. Pe baza codului Baudot, alfabetul Morse al teleimprimatoarelor, Vernam a avut ideea de a construi o maşină care să asigure cifrarea şi descifrarea automată. În codul Baudot, numit aşa după numele inventatorului său, fiecare caracter (literă) este compus din cinci unităţi. La rîndul ei, fiecare unitate este reprezentată de semne sau spaţii, în funcţie de existenţa sau non-existenţa curentului electric la un moment dat. Se obţin, deci, 32 de combinaţii de semne şi spaţii. Fiecare asemenea combinaţie este echivalentă cu cîte o literă. Printr-un aranjament electric, aplicînd rotirea comutatorilor, cînd o anumită literă de pe tabloul alfabetic este apăsată, se transmite secvenţa corespunzătoare de semne şi spaţii. De exemplu : *a* este egal cu semn-semn-spaţiu-spaţiu-spaţiu ; *i* este egal cu spaţiu-semn-semn-spaţiu-spaţiu.

La celălalt capăt al firului, curentul electric încarcă nişte electromagneţi care, prin combinaţii, selectează litera adecvată şi o imprimă. În banda de hîrtie folosită în teleimprimatoare doar semnele sînt reprezentate prin găuri. Ca să citească banda, nişte cuie de metal intră prin găuri şi completează un circuit electric transmiţînd impulsurile de curent. Unde este spaţiu,

hîrtia nu permite închiderea circuitului, iar curentul electric nu trece prin electromagneţi. Ca atare, hîrtia rămîne intactă.

Vernam a sugerat ca pe o bandă de hîrtie să fie transmisă o cheie formată din semne şi spaţii, care să se adune, în mod electromecanic, cu impulsurile textului clar, suma urmînd să constituie criptograma. Adunarea trebuie să fie reversibilă, în aşa fel încît maşina receptoare să poată scădea impulsurile ce formau cheia şi să redea numai textul clar. Vernam a stabilit următoarea regulă : dacă cheia şi impulsurile textului clar sînt (ambele) semne sau spaţii, impulsul textului cifrat să fie spaţiu. Dacă impulsul cheii este spaţiu şi impulsul textului clar semn ori viceversa sau, cu alte cuvinte, cele două simboluri sînt diferite, impulsul textului cifrat va fi un semn. Cele patru posibilităţi, în formulă matematică, sînt :

text clar		*cheie*		*text cifrat*
semn	+	semn	=	spaţiu
semn	+	spaţiu	=	semn
spaţiu	+	semn	=	semn
spaţiu	+	spaţiu	=	spaţiu

Descifrarea nu dă naştere la ambiguităţi. De exemplu, dacă textul cifrat este semn şi cheia spaţiu, în textul clar este posibil să apară numai semnul.

Întregul sistem poate fi aranjat într-un singur tabel. Folosind transcrierea convenţională *1* pentru semn şi *0* pentru spaţiu, regula poate fi exprimată astfel :

		text clar 1	text clar 0	
cheia	1	0	1	text cifrat
	0	1	0	

Conform cu această regulă, Vernam a combinat cele cinci unităţi ale caracterelor clare cu cele ale cheii şi a obţinut cinci unităţi de caractere cifrate. Astfel, dacă textul clar este *a* sau 11000, iar cheia este 10011, textul cifrat este următorul :

text clar : 11000
cheia : 10011
text cifrat : 01011

Textul clar obţinut de corespondent a rezultat din combinarea care a avut loc prin aplicarea impulsurilor care constituie cheia peste impulsurile textului clar. De exemplu, dacă text cifrat = 10100, cheia = 00110 se obţine :

text cifrat : 10100
cheie : 00110
text clar : 10010 sau litera d

Ca să combine electric impulsurile, Vernam a inventat un dispozitiv din magneţi, relee şi bobine. Cum cifrarea şi descifrarea erau reciproce, acelaşi aparat era folosit pentru ambele operaţii.

În aparat erau introduse două benzi — una pe care era cheia şi cealaltă pe care era textul. Cînd unităţile de pe cele două benzi erau identice se deschidea un circuit şi apărea un spaţiu, iar cînd erau diferite se închidea circuitul şi apărea un semn. Semnele şi spaţiile rezultate se transmiteau, ca orice alt mesaj teleimprimat, la corespondent, unde aparatul Vernam scădea unităţile cheii, furnizate de o bandă similară cu cea a expeditorului şi astfel se obţinea textul clar. Automat, banda obţinută se transmitea la o maşină de teleimprimat şi, în felul acesta, se obţinea mesajul direct în clar.

Deci, nu mai era nevoie de cineva care să cifreze sau să descifreze texte (deşi benzile cheie erau confecţionate în continuare). Toate aceste operaţii se făceau mecanic. Se introducea în maşină text clar şi se obţinea text clar, cu aceeaşi viteză cu care se transmite şi se recepţionează orice mesaj în limba engleză. Dacă cineva interceptează astfel de mesaje obţine doar secvenţe care n-au nici un înţeles (semne şi spaţii). Avantajul principal al acestui sistem este acela că eliberează procesul criptografic de necesitatea unui timp mai mare pentru scrierea unor asemenea mesaje, iar posibilitatea ivirii erorilor este aproape egală cu zero. De asemenea, a fost eliminat cifrorul din cadrul comunicaţiilor, activitatea acestuia fiind automatizată.

Aceste calităţi i-au fost repede recunoscute aparatului Vernam şi metodele de criptare pe care le implica s-au dez-

voltat rapid. În primele zile, cheile pentru acest aparat aveau forma unor rotoare cu benzi de hîrtie pe care erau imprimate semne trase din pălărie, obținîndu-se astfel chei întîmplătoare. Dar inginerii, care au învățat repede criptologie, și-au dat seama de faptul că acesta nu putea fi un sistem științific și au făcut o asemănare între el și alte sisteme polialfabetice. Cu ajutorul codului Baudot, se poate forma un tablou de 32 x 32 în care șirul de deasupra să fie textul clar, iar prima coloană cheia.

Întrucît secretul sistemului lui Vernam rezida mai ales în cheie, s-a recurs la folosirea de chei foarte lungi care, pe lîngă avantajele pe care le aveau, prezenta și unele inconveniente, în sensul că benzile erau greu de manipulat. De aceea, un alt inginer, cu numele de Morshouse, a recurs la combinarea de două chei scurte într-un aparat Vernam, ca și cum una ar fi servit la cifrarea celeilalte. Rezultatul obținut : o bandă foarte lungă care servea drept cheie pentru textul clar. Acest tip de cheie s-a numit cheie secundară. Lungimea ei provenea din diferența de semne din cheile primare. De exemplu, dacă cele două chei primare înregistrate conțineau una 1 000 de caractere, iar cealaltă 999, diferența de un singur caracter dădea naștere la 999 000 de combinații. Astfel, două benzi de aproximativ 4 m fiecare dădeau naștere unei chei care, pentru a putea fi înregistrată, erau necesari peste 4 000 metri de bandă. Aceasta a fost una din cele mai de seamă îmbunătățiri.

Totuși, nici acest sistem nu putea fi considerat ca imun în fața criptanaliștilor căci orice repetare, de orice fel, a cheii în criptograme, la o analiză sistematică, poate pune în pericol secretul mesajului, dînd posibilitatea de soluționare.

Nu contează dacă repetarea se face în același mesaj sau în mesaje diferite și nici dacă are loc, mai ales datorită interacțiunii dintre cheile primare sau simplei repetări a unei chei lungi. Ca să se evite pericolul repetiției și neajunsul inteligibilității, cheile trebuie să nu aibă sfîrșit și sens. În felul acesta, Mauborgne, un alt criptanalist, a sintetizat într-un singur tip de cheie hazardul (cheia întîmplătoare) lui Vernam și non-repetiția descoperită de criptologii Școlii militare americane de

comunicații. Așa s-a născut cheia folosită o singură dată. Caracteristica acestui procedeu constă în aceea că o cheie este aleasă la întîmplare și este folosită o singură dată. Acest fapt asigură un nou și neprevăzut caracter pentru fiecare mesaj din totalul de mesaje trimise de un grup de corespondenți.

Un astfel de sistem nu poate fi soluționat nici în teorie, nici în practică, indiferent de cantitatea de text și de timpul pe care îl are criptanalistul la dispoziție, pentru că asta înseamnă să adune toate literele cifrate cu ajutorul unui singur alfabet și să le studieze caracterele lingvistice. În acest sens, există mai multe metode. Una dintre ele este metoda Kasiski care constă din selecționarea literelor cifrate identic, folosindu-se o cheie ce se repetă. Un text cifrat cu o cheie continuă, formată dintr-un text coerent, poate fi soluționat reconstruindu-se reciproc textul clar și textul-cheie. O cheie continuă cu text luat la întîmplare, folosit în două sau mai multe mesaje, se rezolvă printr-o reconstrucție simultană a celor două texte clare, ajutînd, totodată, la verificarea reciprocă a soluțiilor. Alte sisteme polialfabetice, cum ar fi autocheia și sistemul celor două benzi, pot fi soluționate prin metode care își au originea în particularitățile lor. Literele cifrate monoalfabetic sînt țelul urmărit de orice criptanalist care folosește metodele descrise. Sistemul Vernam conține în sine acest tip de substituție, deoarece cele 32 de alfabete de cifrat sînt folosite în mod repetat. Dar criptanalistul nu are cum să ajungă la ele, deoarece cheia folosită doar o singură dată nici nu se repetă, nici nu revine, nici nu are sens, nici nu dă naștere la schelete interne. Prin urmare, toate metodele criptanalistului bazate, într-un fel sau altul, pe aceste caracteristici nu dau rezultate. Caracterul întîmplător al cheilor folosite o singură dată reduce la zero orice comparație de lungime sau coerentă de tipul celor găsite în autochei. De asemenea, acest gen de cheie, datorită faptului că este folosită o singură dată, împiedică formarea coloanelor verticale ale lui Kasiski sau Kerckhoffs, cum este cazul cheilor repetate într-unul sau mai multe mesaje. Cu alte cuvinte, criptanalistul este blocat.

Dar mai există teoria probabilităților, calculul erorilor. S-ar părea că încercarea directă a tuturor cheilor posibile, una după alta, ar putea duce la textul clar. Succesul obținut pe această cale e o iluzie, deoarece va fi foarte greu să alegi din noianul de texte de aceeași lungime, descoperite prin această metodă, pe cel bun. Să presupunem că un criptanalist descifrează un mesaj militar format din patru litere, luînd la rînd toate cheile, începînd cu AAAA. Textul clar obținut cu cheia AABI ar fi kiss (sărut). Nu este cel căutat. Merge mai departe. AAEL dă kill (a ucide). Începe să fie pe drumul cel bun, dar vrea să fie sigur și continuă. Cheia AAEM dă kilt (fustă scoțiană). Acest cuvînt poate însemna o referire la o manevră a scoțienilor. AAER dă kiln (cazan de țuică). Obține apoi cuvintele fast (repede) cu cheia LZBM, slow (încet) cu KHIA, stop cu HRIW, gogo (merge, merge) cu XSTT, hard (greu, tare, dur) cu PZVQ și easy (ușor) cu RZBU. Cînd termină cu ZZZZ își dă seama că a reușit să compileze o listă de cuvinte formate din patru litere și nimic mai mult. Cuvintele obținute astfel le poate extrage și dintr-un dicționar, dar cum să descopere care este adevăratul mesaj pe care îl conțin ?! Cheia nu ajută la limitarea alegerii, deoarece, avînd un caracter întîmplător, fiecare grup de patru litere este tot atît de acceptabil ca cheie ca și oricare altul. Soluționarea devine cu atît mai grea cu cît mesajul este mai lung, deoarece și numărul soluțiilor posibile crește. Există numai trei soluții posibile pentru o criptogramă formată dintr-o singură literă, dar sînt zeci pentru cele formate din două și trilioane pentru cele formate dintr-o sută de litere !

Chiar dacă intrăm în posesia cheii unei criptograme n-o putem extinde și la decriptarea altui text criptat, deoarece aceasta nu se folosește decît o singură dată.

Acestea sînt dovezi empirice. Este, totuși, posibil să demonstrăm științific că acest sistem este infailibil. Iată și dovada teoretică că într-adevăr este așa. În esență, cifrarea în sistemul Vernam este o adunare simplă, bazată pe alfabetul Baudot. Să presupunem, deci, că textul clar este 4, iar cheia este 5. Textul cifrat va fi 9. Avînd doar această cifră, criptanalistul n-are cum să știe că 9 este rezultatul lui 7 + 2 sau 6 + 3

sau 11 — 2 sau 4 + 5 ori al oricărei alte adunări din cele 32 de combinații posibile. Generalizînd, obținem ecuația $x + y = 9$. Aceasta este o ecuație cu două necunoscute și pentru rezolvare sînt necesare două ecuații cu aceleași necunoscute, or cheia întîmplătoare folosită o singură dată îl împiedică pe criptanalist să facă acest lucru. Din cele 32 soluții pentru chei și 32 soluții pentru textul din cazul nostru, unele sînt mai probabile decît altele. Astfel, soluția unei litere poate fi *e* în proporție de 12%, *t* de 8% etc., conform cu tabelul frecvenței. Dar această probabilitate nu dă răspuns întrebării pe care și-a pus-o criptanalistul, deoarece nu-i arată care dintre aceste probabilități se află în momentul respectiv în fața lui !

Folosirea acestui sistem este deosebit de dificilă în situații cînd se cere transmiterea unui volum mare de mesaje, deoarece sînt necesare enorm de multe chei de același tip pentru ambii corespondenți și, de aceea, este practic imposibil de folosit pe cîmpul de luptă între unități și subunități. Producerea de chei pentru toate mesajele cere mult timp și cheltuielile pe care le implică sînt foarte mari, dar aceste dificultăți nu se întîlnesc în situații mai stabile, cum ar fi cazul marilor comandamente militare, corpurilor diplomatice sau corespondenței între doi spioni. În astfel de cazuri acest sistem este destul de practic și foarte mult folosit, deși atunci cînd volumul de mesaje este foarte mare apar greutăți.

Există și un alt sistem de cifrare care are la bază operațiuni matematice. De-a lungul vremurilor, mulți matematicieni au cochetat cu această idee, dar profesorul american Hill a fost primul care a folosit cu succes algebra în criptografie. Hill a pus la punct o metodă generală care a făcut, pentru prima dată, ca criptografia poligramelor să poată fi folosită în practică.

Metoda se folosește de ecuații în care cheia și literele din textul clar au valori numerice. Cifrarea constă din rezolvarea ecuațiilor. Există un număr de ecuații egal cu numărul de litere din text. Deoarece există douăzeci și șase de litere în alfabet și pentru ca și descifrarea să fie posibilă, Hill a făcut calculele modulo 26. Asta înseamnă că criptograful folosește doar numere

7 c. 144

de la 0 la 25, orice număr mai mare decît 25 trebuie redus modulo 26. Astfel, 28 este congruent cu 2 modulo 26, deoarece 28 — 26 = 2. La fel 68 este congruent 16, modulo 26, deoarece 68 : 26 = 2, rest 16.

Pentru a demonstra cum funcționează sistemul inventat de el, Hill a înlocuit literele textului clar cu x, iar literele textului cifrat cu y în ordinea x_1 = prima literă, x_2 cea de-a doua ș.a.m.d. A ajuns, astfel, la următoarele ecuații :

$$y_1 = 8x_1 + 6x_2 + 9x_3 + 5x_4$$
$$y_2 = 6x_1 + 9x_2 + 5x_3 + 10x_4$$
$$y_3 = 5x_1 + 8x_2 + 4x_3 + 9x_4$$
$$y_4 = 10x_1 + 6x_2 + 11x_3 + 4x_4$$

Cînd a început cifrarea unui text ca acesta : „Delay operations" (întîrziați operațiunile — N.T.), Hill a transformat literele din textul clar în numere luate la întîmplare, ca în exemplul de mai jos :

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t
5	23	2	20	10	15	8	4	18	25	0	16	13	7	3	1	19	6	12	24

u	v	w	x	y	z
21	17	14	22	11	9

Apoi a luat valorile numerice ale primelor patru litere din textul clar, în cazul nostru „dela", și le-a trecut în locul lui x_1, x_2, x_3, x_4 din ecuațiile de mai sus. Procedînd astfel, a ajuns la următoarea formulă :

$$y_1 = (8 \times 20) + (6 \times 10) + (9 \times 16) + (5 \times 5)$$
$$y_2 = (6 \times 20) + (9 \times 10) + (5 \times 16) + (10 \times 5)$$
$$y_3 = (5 \times 20) + (8 \times 10) + (4 \times 16) + (9 \times 5)$$
$$y_4 = (10 \times 20) + (6 \times 10) + (11 \times 16) + (4 \times 5)$$

În continuare, Hill a făcut înmulțirile și adunările aplicînd regula modulo 26. De exemplu, cînd a rezolvat pe y_1 a obținut 8 x 20 = 160; 160 : 26 = 6, rest 4. Deci 8 x 20 = 4; la fel a făcut toate celelalte operații 6 x 10 = 8, 9 x 16 = 14 și 5 x 5 = 25.

Rezultatul final al adunării este 51. Deci, aplicînd modulo 26, obținem 25, care, în alfabetul nostru, este egal cu litera j. Celelalte litere sînt aflate în același fel și textul cifrat pentru „dela" devine JCOW, iar criptograma completă este JCOW ZLVB DVLE QMXC.

Să presupunem că textul clar începe cu cuvîntul Demand (cereți)..., care are schimbată, doar cea de-a treia literă față de prima criptogramă și anume, în loc de *l* avem *m*. Înlocuirea în cele patru ecuații a lui 16, echivalentul lui *l*, cu 13, echivalentul lui *m*, schimbă rezultatele pentru toate celelalte elemente ale ecuației și, în consecință, textul cifrat pentru „dema", care este CMZQ, este cu totul diferit de JCOW al lui „dela". Un asemenea sistem este cu adevărat polialfabetic, iar rezistența lui criptografică este substanțială.

Valorile fixe în ecuații — numerele cu care se înmulțesc numerele literelor din textul clar — nu pot fi selecționate la întîmplare, dacă vrem ca sistemul să fie reversibil. Hill a specificat aceste cerințe și a formulat și ecuațiile de descifrare. Pentru cazul nostru, aceste ecuații sînt :

$$x_1 = 23y_1 + 20y_2 + 5y_3 + 1y_4$$
$$x_2 = 2y_1 + 11y_2 + 18y_3 + 1y_4$$
$$x_3 = 2y_1 + 20y_2 + 6y_3 + 25y_4$$
$$x_4 = 25y_1 + 2y_2 + 22y_3 + 25y_4$$

Hill a eliminat însă în cele din urmă ecuațiile de descifrare, construind „transformările involutorii". Un singur set de asemenea ecuații servește atît la cifrare cît și la descifrare. Aceste „transformări involutorii" sînt construite cu ajutorul unei formule speciale, care limitează numărul ecuațiilor. În teorie, acest fapt reduce rezistența criptanalistică a textului cifrat, dar reducerea este neînsemnată, în special dacă o comparăm cu proporția în care ne ușurează operațiunea.

Operațiunea de cifrare a fost ușurată și mai mult prin introducerea matricelor. O matrice nu este altceva decît un pătrat cu numere. Matricele pot fi adunate și înmulțite conform unor reguli proprii, iar numerele de pe matrice reprezintă litere din

textul clar. Şi deoarece fiecare matrice poate fi folosită din punct de vedere aritmetic ca un singur număr, două ecuaţii pot servi la cifrarea a două matrice, indiferent cîte numere conţine fiecare. Astfel, prin dispunerea textului clar pe matrice, mai multe litere pot fi cifrate folosind foarte puţine ecuaţii. De exemplu, două matrice de 3 x 3 cifrează 18 litere, folosind doar două ecuaţii, în loc de 18, cîte ar fi fost necesare pentru o cifrare simplă sau liniară.

Hill a prezentat următorul exemplu pentru a-şi explica teoria : Hold up. Supporting air squadrons en route (Rezistaţi. Escadrile aeriene de ajutor sînt în drum spre voi), folosind de data aceasta un alfabet numeric diferit de primul şi pregătindu-şi matricele în felul următor : (matricea 1 = x_1; matricea 2 = x_2);

$$x_1 = \begin{matrix} h & o & l \\ d & o & u \\ t & s & u \end{matrix} = \begin{matrix} 5 & 6 & 22 \\ 2 & 6 & 7 \\ 12 & 19 & 7 \end{matrix}$$

$$x_2 = \begin{matrix} p & p & o \\ r & t & i \\ n & g & a \end{matrix} = \begin{matrix} 21 & 21 & 6 \\ 23 & 12 & 17 \\ 24 & 16 & 4 \end{matrix}$$

Pe acestea le-a înlocuit în ecuaţii şi a mai alcătuit o matrice arbitrară pentru a complica şi mai mult descifrarea.

$$y_1 = \begin{matrix} 3 & 6 & 2 \\ 16 & 23 & 8 \\ 2 & 16 & 13 \end{matrix} \cdot \begin{matrix} 5 & 6 & 22 \\ 2 & 6 & 7 \\ 12 & 19 & 7 \end{matrix} + \begin{matrix} 2 & 6 & 14 \\ 8 & 24 & 4 \\ 14 & 16 & 20 \end{matrix} \cdot \begin{matrix} 21 & 21 & 6 \\ 23 & 12 & 18 \\ 24 & 16 & 4 \end{matrix} + \begin{matrix} 18 & 6 & 6 \\ 24 & 20 & 26 \\ 2 & 2 & 16 \end{matrix}$$

$$y_2 = \begin{matrix} 18 & 14 & 22 \\ 20 & 4 & 10 \\ 22 & 20 & 24 \end{matrix} \cdot \begin{matrix} 5 & 6 & 22 \\ 2 & 6 & 7 \\ 12 & 19 & 7 \end{matrix} + \begin{matrix} 15 & 16 & 20 \\ 4 & 13 & 2 \\ 20 & 8 & 11 \end{matrix} \cdot \begin{matrix} 21 & 21 & 6 \\ 23 & 12 & 17 \\ 24 & 16 & 4 \end{matrix} + \begin{matrix} 2 & 16 & 14 \\ 8 & 12 & 4 \\ 18 & 8 & 20 \end{matrix}$$

După ce a făcut toate operaţiunile, înmulţiri şi adunări, şi a aplicat modulo 26, a obţinut următoarele rezultate :

$$y_1 = \begin{matrix} 13 & 20 & 12 \\ 22 & 16 & 23 \\ 16 & 19 & 23 \end{matrix} = \begin{matrix} Y & K & T \\ L & G & R \\ G & S & R \end{matrix} \qquad y_2 = \begin{matrix} 13 & 23 & 12 \\ 17 & 20 & 15 \\ 20 & 4 & 20 \end{matrix} = \begin{matrix} Y & R & T \\ I & K & W \\ K & A & K \end{matrix}$$

O asemenea cifrare aproape că exclude posibilitatea unor repetiţii. O cifrare polialfabetică de această mărime este posibilă numai cu ajutorul transformărilor Hill. Din punct de vedere matematic nu există nici o limită atît pentru mărimea matricelor cît şi pentru numărul de ecuaţii. Se pot folosi matrice cu latura pătratului de 10 litere, iar cu ajutorul a numai cinci ecuaţii se poate cifra un text de 500 de litere.

Din punct de vedere practic, matricea e mai avantajoasă, deoarece ajută la cifrarea unui număr mai mare de litere, dar cifrarea liniară, folosind mai multe chei arbitrare, asigură aceluiaşi text o rezistenţă mai mare.

Deci, acest sistem face ca o astfel de criptogramă să nu poată fi atacată decît dacă criptanalistul dispune de alfabetul iniţial.

Dacă cunoaşte alfabetul şi reuşeşte să intre în posesia a două criptograme ale aceluiaşi text, dar cifrat cu ecuaţii deosebite, atunci obţine uşor ecuaţiile de cifrare.

Deşi acest sistem elaborat de Hill nu a fost şi nu este prea mult folosit, meritul lui constă în faptul că a dezvăluit fondul matematic al criptologiei. Criptologia contemporană este saturată de operaţiuni matematice, metode matematice, gîndire matematică. În practică, criptologia a devenit o simplă ramură a matematicii aplicate.

Istoria ştiinţei este plină de coincidenţe. Ea cunoaşte multe cazuri cînd o descoperire este făcută în acelaşi timp de unul sau mai mulţi oameni. Acesta este şi cazul criptologiei.

Patru oameni, din patru ţări diferite, sub imboldul dat de folosirea intensă, în timpul primului război mondial, a comunicaţiilor secrete şi de dezvoltarea mecanizării, în mod cu totul şi cu totul independent, au creat maşina al cărei principiu se foloseşte cel mai mult în criptografia din zilele noastre. Principiul este acela al roţii de cod bobinate sau mai pe scurt al rotorului.

Corpul rotorului, fabricat din material izolant cum ar fi bachelita sau cauciucul, de obicei, are un diametru de 5—8 cm şi o grosime de 1 cm. Pe circumferinţa rotorului se găsesc tra-

sate 26 de contacte electrice, așezate la distanțe egale. Aceste contacte sînt, de regulă, fabricate din aramă sau alamă. Fiecare contact este legat la întîmplare cu un contact de pe partea opusă, astfel încît se stabilește o legătură electrică între două puncte opuse situate pe circumferință. Contactele de la intrarea curentului în rotor formează literele textului clar, iar contactele de la ieșire, literele textului cifrat. Firul electric care leagă cele două contacte opuse asigură transformarea literelor textului clar în text cifrat.

Pentru a cifra un mesaj se conectează o sursă de curent electric la rotor, la contactul de intrare a literei pe care vrem să o cifrăm, să zicem *a*. Curentul trece de-a lungul firului și ajunge la contactul de pe partea opusă, care reprezintă, să zicem, litera *R*. Dacă se face o listă cu toate legăturile de pe cele două părți, se obține un alfabet de substituție simplă. În felul acesta, rotorul conține un alfabet de cifrat sub o formă care se pretează la manipulare electromecanică.

Pentru a se putea executa o asemenea manipulare, rotorul a fost plasat între două plăci fixe, fiecare placă fiind fabricată din material izolant și avînd 26 de contacte fixate sub formă de cerc, în așa fel încît să se potrivească cu cele de pe rotor. Fiecare contact de pe placa de intrare a curentului este conectat la literele unei mașini de scris care reprezintă literele textului clar. Contactele de pe placa de ieșire sînt conectate la un tablou pe care, cu ajutorul unui beculeț, se indică litera din textul cifrat. Cînd cifrorul apasă pe cheia ce reprezintă litera *a*, el permite curentului electric să treacă de la sursă la placa de contact pentru *a*, de aici în rotor la contactul literei *a* și, prin firul de legătură, la litera *R* de pe partea cealaltă, adică la litera de cifrat, iar de acolo la contactul *R* aflat pe placa de ieșire și, în continuare, la becul care luminează litera *R* de pe tabloul de cifrare.

Dacă totul s-ar fi redus la aceasta, atunci întregul mecanism ar fi constituit doar o mașină scumpă cu ajutorul căreia se execută o substituție simplă. În practică însă, rotorul nu rămîne pe loc, ci se învîrtește. Să presupunem că se mișcă doar cu un singur contact și apăsăm din nou pe litera *a*, de data

aceasta litera de cifrat n-are să mai fie *R*, ci cu totul alta, datorită noului contact de pe rotor, care are pe partea cealaltă o altă literă de contact. De asemenea, toate celelalte litere din textul clar au drept corespondente alte litere de cifrat sau, cu alte cuvinte, de fiecare dată se folosește un alt alfabet de cifrat. Se poate face o listă a acestor alfabete, deoarece toate sînt bazate pe alfabetul primar al rotorului și, prin urmare, se va obține tabloul de 26 x 26, bazat pe un singur alfabet mixt, avansînd cu o literă la fiecare nou alfabet. Aceasta înseamnă că am obținut doar o substituție polialfabetică cu cheie progresivă, avînd la bază un alfabet mixt de 26 de litere. Bineînțeles că nici acest lucru n-ar fi justificat construcția mașinii. Totuși, dacă se mai pune un rotor lîngă primul, schimbarea este esențială, deoarece se vor produce două cifrări succesive. Dacă rotoarele se învîrt simultan, rezultatul va fi și în continuare o substituție polialfabetică bazată pe un alfabet mixt, dar dacă cel de-al doilea rotor se mișcă numai o singură dată, în timp ce primul rotor execută o mișcare de rotație completă, schimbarea va fi fundamentală. Această nouă poziție aduce în joc un nou alfabet de cifrat, cel de-al 27-lea. Fiecare schimbare de poziție între cele două rotoare și a acestora față de plăcile statoare dă naștere unui nou alfabet de cifrat.

Dacă mașina se construiește în așa fel încît pentru fiecare rotație completă a primului rotor cel de-al doilea se mișcă doar cu un spațiu, primul rotor efectuează 26 de rotații, în timp ce cel de-al doilea execută doar una; rezultatul obținut justifică cheltuielile făcute pentru construirea mașinii. Întrucît cel de-al doilea rotor are 26 de poziții și primul rotor se oprește pentru fiecare poziție de 26 de ori, se obțin 676 de poziții diferite față de plăcile statoare. Cele 676 de poziții înseamnă 676 de alfabete de cifrat diferite.

Adăugînd un al treilea rotor, se obțin 17 576 alfabete, cu al patrulea 456 976, iar cu al cincilea 11 881 376!

În acest număr uriaș de alfabete stă puterea sistemului rotor, fiecare literă fiind cifrată în cu totul și cu totul alt alfabet. Sistemul diferă de sistemul Vernam în care s-ar folosi o cheie cu 11 881 376 caractere, deși perioada este aceeași. Deose-

birea constă în aceea că Vernam folosește doar 32 de alfabete, iar secretul rezidă în lipsa totală a repetărilor, în succesiunea în care sînt folosite. Rotoarele se mişcă într-o ordine rigidă care poate fi prevăzută, fapt ce micşorează rezistenţa textelor cifrate şi, în plus, după folosirea tuturor alfabetelor, perioada se repetă. Totuşi, rotoarele lucrează cu asemenea lungimi astronomice încît o diferenţă de un grad schimbă totalmente natura mesajului. Meritul rotoarelor este acela de a produce alfabete diferite pentru fiecare literă dintr-un text clar mai lung decît operele complete ale lui Shakespeare, romanul Război şi pace, Iliada, Odiseea etc.

O asemenea perioadă de repetiţie înlătură orice soluţionare directă pe baza frecvenţei literelor, întrucît o soluţie generală de acest gen ar necesita 50 de litere pentru fiecare alfabet de cifrat, ceea ce înseamnă că toate cele cinci rotoare trebuie să parcurgă ciclurile lor combinate de 50 de ori. Criptograma ar totaliza cam tot atîtea pagini cît totalizează toate luările de cuvînt din Congresul şi Senatul american de-a lungul a trei sesiuni consecutive. Chiar dacă ar aduna o viaţă întreagă, criptanalistul tot n-ar obţine o asemenea cantitate de mesaje.

De aceea, criptanalistul caută cazuri deosebite care să-i permită soluţionarea criptogramelor din sistemul rotor. Astfel, el poate repurta succese în diferite moduri. Dacă cîteva mesaje încep din aceeaşi poziţie a rotorului sau din poziţii foarte apropiate încît să apară secvenţe ale alfabetului de cifrat, poate folosi metoda suprapunerii lui Kerckhoffs. Uneori cuvinte probabile sau începuturi stereotipe dau unele indicaţii, iar alteori, datorită neglijenţei cifrorului sau publicării unor note diplomatice etc., se obţine soluţia pentru întregul sistem. Toate aceste lucruri se întîmplă destul de des şi criptanaliştii le exploatează.

De asemenea, se folosesc diferite metode matematice, în special teoria grupurilor, care se potriveşte foarte bine pentru rezolvarea ecuaţiilor cu mai multe necunoscute, cum este cazul soluţiilor la criptogramele bazate pe sistemul rotor. În fond, necunoscute sînt doar legăturile de la contactele de pe o parte

a rotorului cu cele de pe partea opusă. Matematicianul criptanalist, pentru a afla numărul lor, măsoară distanţa dintre contactele de intrare şi cele de ieşire.

De exemplu, un fir de la contactul de intrare 3, care iese prin contactul de ieşire 10, marchează o distanţă de 7 contacte. În mod similar, literele primesc valori numerice, de obicei $a = 0$, $S = 1$ ... $z = 25$. Folosind valorile cunoscute sau presupuse ale literelor clare, criptanalistul formează ecuaţii în care distanţele de pe rotor constituie necunoscutele pe care le află rezolvînd ecuaţiile în mod matematic.

De pildă, criptanalistul găseşte două litere identice în cuprinsul primelor 26 de litere din criptogramă. În această etapă doar primul rotor se mişcă, celelalte patru rămîn nemişcate. Deoarece două impulsuri electrice au ajuns la aceeaşi literă, înseamnă că au trebuit să străbată acelaşi circuit prin toate cele patru rotoare. Circuitul a fost altul doar în primul rotor. Criptanalistul face două ecuaţii. În fiecare din aceste ecuaţii, valoarea numerică a textului cifrat este egală cu valoarea cunoscută sau presupusă a textului clar plus distanţele necunoscute de pe primul rotor şi distanţele necunoscute de pe celelalte patru rotoare. El ia în consideraţie, printr-o corecţie, faptul că primul rotor s-a mişcat de un număr de ori. Rezolvă apoi după toate regulile algebrei cele două ecuaţii. În cazul acesta, efectul celorlalte rotoare este redus la zero, deoarece prima operaţiune este scăderea. Valoarea numerică obţinută prin rezolvarea ecuaţiilor este egală cu diferenţa dintre cele două contacte de pe primul rotor. Repetînd operaţiunea, criptanalistul poate afla diferenţa dintre mai multe contacte opuse de pe primul rotor şi, pe această bază, construieşte legăturile, consecinţa logică fiind descifrarea primelor 26 de litere din criptogramă.

În mod similar se reconstruieşte şi cel de-al doilea rotor. Pentru a reuşi acest lucru trebuie neutralizate mişcările celorlalte. Astfel, primul rotor trebuie să fie întotdeauna în aceeaşi poziţie şi anume : prima, a douăzeci şi şaptea, a cincizeci şi treia etc., iar literele obţinute sînt cele 26 aflate pe rotorul al doilea. La fel se procedează şi cu celelalte rotoare, alegîndu-se perioadele adecvate.

Acestea sînt principiile de bază ale soluționării sistemului rotor, dar, așa cum vă puteți da seama, sistemul rotor produce totuși un cifru extrem de complex și de rezistent.

Cei patru inventatori ai rotorului de cifrat au fost americanul Edward Hugh Hebern, olandezul Hugo Alexander Koch, germanul Arthur Scherbius și suedezul Arvid Gerhard Damm.

După cel de-al doilea război mondial, milionarul suedez Hagelin, unul dintre cei care au perfecționat mașina de cifrat, a pus bazele unei firme ce fabrică mașini de cifrat pe care le vinde pe piața internațională. Printre clienții săi se numără peste 60 de guverne din diferite țări, care cumpără aceste mașini atît pentru oficiile diplomatice cît și pentru armată. Instalația completă costă între 30 000 și 50 000 de dolari, iar funcționarii firmei explică tuturor procedeele de funcționare a mașinilor, metodele de stabilire a cheilor, dar se feresc să facă recomandări precise, ca nu cumva clientul să creadă că ele se dau și la alții.

Din modul în care prosperă Hagelin, reiese clar că afacerile sînt rentabile și „secretul" constituie o afacere bănoasă.

CENZORI ȘI SPIONI

Cifrul este limba spionilor care, de obicei, vorbesc în șoaptă. Pentru ca acțiunile unui spion să fie încununate de succes este necesar ca el să nu fie văzut și auzit. Trimiterea de mesaje sub formă criptografică ar pune în stare de alertă contraspionajul și soarta spionului ar fi repede pecetluită. Totuși, el trebuie să transmită informațiile pe care le are, altfel existența sa nu este justificată. Așa se face că el recurge la metode subtile de a ascunde chiar și faptul că a fost trimis un mesaj secret. Pentru a bloca această posibilitate cît și pentru a descoperi dușmanul care a pătruns în interior, guvernele tuturor țărilor au construit filtre pentru a preveni și detecta comunicările secrete. Aceste filtre, care lasă să treacă numai mesajele nevinovate, nu sînt altele decît organele de cenzură.

În continuare, vor fi prezentate cîteva din metodele folosite de către spioni în comunicările secrete și procedeele de depistare a lor.

În special, în timp de război se impun o serie de restricții asupra corespondenței, pentru a se pune o primă stavilă în calea metodelor secrete de comunicare. Astfel, se interzic jocurile de șah prin corespondență, jocurile de cuvinte încrucișate, trimiterile de decupări, listele cu diferite grade și titluri universitare și școlare etc. Motivele acestor restricții sînt ușor de înțeles : asemenea trimiteri pot ascunde comunicări secrete, greu de descoperit. Un exemplu în acest sens, destul de hazliu, dar care s-ar

fi putut dovedi absolut necesar, îl constituie cazul reținerii unei scrisori în care se dădeau niște instrucțiuni de tricotat. Serviciul de cenzură american din timpul celui de-al doilea război mondial a reținut această scrisoare pînă cînd o funcționară din cadrul acestui serviciu a confecționat un pulover întreg urmînd instrucțiunile din scrisoare, pentru a vedea dacă în spatele lor nu se ascundea cu totul altceva. Un caz asemănător s-a întîmplat în timpul revoluției franceze, cînd o oarecare doamnă Deforge a „tricotat" numele mai multor dușmani ai republicii.

Scrisorile cu un text neclar, care conțin anumite cifre de afaceri ori care sînt scrise într-o limbă străină uzuală, sînt reținute.

Precauțiuni se iau și în ce privește anunțurile și reclamele. Ziarele sînt avertizate asupra pericolului de a publica anumite reclame sau anunțuri care conțin mesaje secrete. Măsuri speciale trebuie, de asemenea, luate în ceea ce privește posturile de radio, care pot transmite mesaje în cod deschis pentru spioni, submarine sau către centrele de spionaj străine. În Anglia și S.U.A. s-au interzis cu desăvîrșire în timpul celui de-al doilea război mondial transmiterea de interviuri cu oameni de pe stradă, liste de jucării pe care Moș Gerilă le dădea copiilor sau erau de vînzare, anunțuri despre pierderea unor cîini etc.

Aceasta este doar o parte din activitatea de cenzură, cealaltă parte se referă la detectarea altor metode care ar putea fi folosite.

În timpul celui de-al doilea război mondial al New York existau 4 300 de funcționari care se ocupau exclusiv cu activitatea de detectare a scrierilor ascunse din trimiterile poștale. Toate mesajele care conțineau texte oarecum forțate, neîndeajuns de clare, suspecte din anumite puncte de vedere, erau examinate cu maximum de atenție.

Din punct de vedere lingvistic există două metode de a trimite mesaje cu caracter suspect : semagramele și codurile deschise. La rîndul lor, codurile deschise pot fi și ele de trei feluri : codul-jargon, cifrul nul și sistemele geometrice de tipul grătarului. În codul-jargon un anumit cuvînt, de obicei foarte banal, înlocuiește termenul real dintr-un text care se vrea cît

mai obișnuit și nevinovat posibil. Fraze în aparență nevinovate, de tipul „L-am vizitat pe omul cu care ai luat masa săptămîna trecută" sau „Joe a fost dus la spital", pot însemna că Joe a fost arestat etc. De obicei, în asemenea situații este bine să se verifice autenticitatea celor conținute în scrisoare, deoarece, așa cum au dovedit-o multe cazuri, mai ales în timpul celui de-al doilea război mondial, în astfel de scrisori se pot ascunde mesaje deosebit de periculoase. Astfel, proprietara unui magazin de păpuși scria că : „O păpușă stricată, îmbrăcată cu o rochie de culoarea ierbii, va fi reparată pînă la începutul lui februarie". În realitate, prin acest mesaj se comunica că „Crucișătorul ușor Honolulu va fi reparat pînă la începutul lunii februarie".

Cifrul nul constă în aceea că numai anumite cuvinte sau litere din textul respectiv au semnificație pentru adresant, cum ar fi, de exemplu, fiecare al cincilea cuvînt sau prima, a doua etc. literă din fiecare cuvînt și așa mai departe, restul textului servind doar la ascunderea mesajului.

Un astfel de text este următorul :

Apparently neutral's protest is thoroughly discounted and ignored. Isman hard hit. Blockade issue affects pretext for embargo on byproducts, ejecting suets and vegetable oils [1].

Acest text greoi și amuzant al unei telegrame interceptate conținea însă următorul mesaj : Pershing sails from N.Y., june 1. (Nava Pershing pleacă din New York pe întîi iunie). Mesajul îl forma fiecare a doua literă din cuvintele telegramei.

A doua categorie de mesaje ascunse din punct de vedere lingvistic o constituie semagramele (sema în limba greacă = semn). Semagrama este o steganogramă în care textul cifrat este substituit prin orice alt semn, exceptînd literele și numerele. Așa, de exemplu, un desen, reprezentînd două obiecte sau figuri, poate fi făcut din liniile și punctele alfabetului Morse, conținînd și ora la care o anumită acțiune urmează să aibă loc !

---

[1] În limba română : „Se pare că protestul neutrilor nu este luat în seamă. El este complet ignorat. Isman a fost lovit greu. Blocada afectează, pretext pentru embargoul asupra produselor secundare, uleiurile vegetale și altele".

Steganografia tehnologică la început a constat mai ales din depistarea scrierilor făcute cu ajutorul cernelurilor invizibile.

Cernelurile secrete sînt de două feluri : lichide organice și produse chimice simpatice.

Lichidele organice ca urina, laptele, oțetul și sucurile de fructe pot fi făcute vizibile printr-o încălzire ușoară. Deși sînt cunoscute din antichitate și sînt foarte vulnerabile, datorită faptului că pot fi procurate ușor, fiind la îndemîna oricui și oricînd, se folosesc și astăzi.

Cernelurile simpatice sînt soluții din diferite chimicale care, cînd se usucă, devin incolore, dar reacționează, devenind vizibile, cu o altă substanță chimică numită agent. De exemplu, dacă se scrie cu sulfat de fier, nimic nu devine vizibil pînă cînd nu se dă peste scrisoare cu cianură de potasiu și, din reacție, rezultă ferocianura ferică, de culoare albastră; subacetatul de plumb devine vizibil numai în reacție cu sulfhidrat de sodiu; sulfatul de cupru devine vizibil în reacție cu vapori de amoniac etc.

Pentru a testa existența cernelii simpatice, lucrătorul din laborator, cu ajutorul cîtorva pensule, legate într-un mănunchi și înmuiate în agenți diferiți, trage o linie în diagonală peste scrisoare. Se folosesc agenți foarte diferiți, încît deseori apar amprentele și picături de sudoare. Pe de altă parte, anumite cerneluri specifice nu apar, ci rămîn în continuare ascunse. Pentru a înlătura liniile respective, scrisoarea este recondiționată pe cale chimică. Scrisorile sînt verificate, de asemenea, și cu ajutorul razelor infraroșii și ultraviolete.

Diferite scrieri cu ajutorul unor substanțe sînt invizibile la lumina zilei sau a unor becuri, dar devin vizibile la lumină ultravioletă.

Lumina infraroșie poate diferenția scrisul cu culori care nu pot fi distinse la lumina obișnuită, așa cum ar fi, de exemplu, un mesaj scris cu culoare verde pe un timbru verde.

Bineînțeles, împotriva acestor metode de depistare a scrierilor ascunse s-au luat o serie de contramăsuri. Una dintre acestea a fost despicarea în două a foii de hîrtie și scrierea mesajului pe partea interioară, după care cele două părți se relipeau. Cerneala fiind în interior, nici un agent nu o făcea vizibilă. Această metodă a fost descoperită cînd un spion german, neatent, a folosit prea multă cerneală și aceasta a trecut prin hîrtie.

Neajunsul în tehnica cernelurilor simpatice este acela că nu permite trimiterea unui volum mai mare de informații.

O altă metodă de a transmite o cantitate mare de informații este de a puncta toate literele, care constituie un mesaj, dintr-un ziar cu ajutorul unei soluții de antracină în alcool. Punctele sînt invizibile în condiții normale, dar apar cînd sînt expuse la lumină ultravioletă.

În cazul de față, neajunsul este acela că ziarele ajung cu întîrziere la destinație, existînd și pericolul de a se rătăci sau rupe.

Un procedeu deosebit este micropunctul. În 1941, americanii au descoperit primul micropunct, care nu este altceva decît fotografia, redusă la scară, a unui mesaj, document etc.

În faza inițială, tehnica micropunctului implica două etape: la început, se făcea o fotografie a mesajului de mărimea unui timbru, apoi se fotografia din nou această imagine printr-un microscop întors, după care se developa negativul fotografiei. Punctul obținut se lua cu ajutorul unui ac și era înserat în textul mască al scrisorii de dragoste, de afaceri etc.

Primul micropunct descoperit conținea o întrebare demnă de acest eveniment și anume : „Unde se fac experiențe cu uraniu ?“.

CUPRINSUL

Responsabil de carte: căpitan CONSTANTIN GĂDEA
Corector: a.c. RADU STOIAN

Dată la cules 16.XI.1976 B.T. la 31.XII.1976

Tiraj 1 600, din care 1 500 exemplare hîrtie semivelină
şi 100 exemplare hîrtie velină, format 16/61 X 86